ProCurve MSM7xx Controllers CLI

Reference Guide

HP ProCurve MSM7xx Controllers

CLI Reference Guide

Publication Number
5992-5933
May 2009

Applicable Products

MSM710 Access Controller	J9328A
MSM710 Mobility Controller	J9325A
MSM730 Access Controller	J9329A
MSM730 Mobility Controller	J9326A
MSM750 Access Controller	J9330A
MSM750 Mobility Controller	J9327A
MSM760 Access Controller	J9421A
MSM760 Mobility Controller	J9420A
MSM765zl Mobility Controller	J9370A

Trademark Credits
Windows NT®, Windows®, and MS Windows® are US registered trademarks of Microsoft Corporation.

Disclaimer
HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

Hewlett-Packard Company
8000 Foothills Boulevard
Roseville, California 95747-5552
www.procurve.com

Contents

In this Contents section, new to 5.3.x contexts and commands are preceded with an asterisk "*" and formatted in green like this:

* new context
    * new command

1 Introduction

About this guide 1-2
Products covered 1-2
HP ProCurve Product Naming 1-2
Important terms 1-3
Typographical conventions 1-3
Command syntax 1-3
Management tool 1-4
HP ProCurve Networking support 1-4
Before contacting support 1-4
Online documentation 1-5
Configuring CLI support 1-5
SSH client support 1-6
Entering strings 1-6
Context hierarchy 1-7
Sample CLI session 1-8
File transfer 1-8
A. The service controller gets the file using a URL 1-8
B. Send a file to the service controller 1-8

2 CLI commands

View context 2-2
arping 2-2
enable 2-2
iperf 2-2
nslookup 2-2

ping 2-2
ps 2-3
quit 2-3
show license 2-3
show logging filtered 2-3
top 2-3
traceroute 2-3

Enable context 2-4
reboot device 2-4
show certificate 2-4
show certificate binding 2-4
iperf 2-4
ping 2-4
arping 2-5
arp 2-5
end 2-5
quit 2-5
rcapture 2-5
show arp 2-5
show bridge 2-5
show bridge forwarding 2-6
show dns cache 2-6
show interfaces 2-6
* show ip 2-6
show ip route 2-6
show system info 2-6
show ip dhcp database 2-6
show satellites 2-6
* show web content 2-7
show client log 2-7
show radius statistics 2-7
show radius users 2-7
show users 2-7
show discrete pin 2-7
config 2-7
show all config 2-7
controlled network 2-8
show controlled network config 2-8

Config context 2-9
* dhcp public ip default lease period 2-9
* dhcp public ip subnet 2-9
certificate 2-9
certificate binding 2-9
certificate revocation 2-9
end 2-9
factory settings 2-10
interface ethernet 2-10
reboot device 2-10
show certificate 2-10
show certificate binding 2-10
show config factory 2-10
username 2-10
interface ip 2-11
interface pptp client-default 2-11
interface gre 2-11
virtual ap 2-11
show subscription plan 2-11
subscription plan 2-11
* mac list 2-12
* show mac list 2-12
ipsec policy 2-12
* admin local authentication 2-12
* admin radius authentication 2-12
* admin radius authentication server 2-12
ip http port 2-13
ip https port 2-13
snmp-server trap certificate-expired 2-13
snmp-server trap certificate-expires-soon 2-13
snmp-server trap web-fail 2-13
snmp-server trap web-login 2-14
snmp-server trap web-logout 2-14
web admin kickout 2-14
web allow 2-14
world-mode dot11 country code 2-14
web access internet-port 2-15
web access lan-port 2-15
web access interface vlan 2-15

web access interface gre 2-15
web access lan 2-15
web access vpn 2-15
dhcp mode 2-16
dhcp server 2-16
dhcp server default domain name 2-16
dhcp server default lease period 2-16
dhcp server default permanent lease period 2-16
dhcp server controller 2-16
dhcp server controller discovery 2-16
dhcp server logout html user 2-17
dhcp server access centralized clients 2-17
dhcp server access lan 2-17
dhcp relay 2-17
* dhcp relay circuit id 2-17
* dhcp relay remote id 2-18
dhcp relay access centralized clients 2-18
dhcp relay access lan 2-18
dhcp relay extend internet port 2-18
clock 2-18
* clock auto adjust dst 2-19
clock timezone 2-19
* clock use custom dst rules 2-19
ntp protocol 2-19
ntp server 2-19
* clock custom dst begins 2-19
* clock custom dst begins format 2-20
* clock custom dst ends 2-20
* clock custom dst ends format 2-20
ntp server 2-21
ntp server failure trap 2-21
config-update automatic 2-21
config-update operation 2-21
config-update time 2-21
config-update uri 2-22
config-update weekday 2-22
snmp-server trap config-change 2-22
snmp-server trap config-update 2-22
logging destination 2-22

snmp-server trap syslog-severity 2-23
snmp-server 2-23
snmp-server access port-1 2-23
snmp-server allow 2-23
snmp-server chassis-id 2-23
snmp-server contact 2-24
snmp-server heartbeat period 2-24
snmp-server location 2-24
snmp-server port 2-24
snmp-server readonly 2-24
snmp-server readwrite 2-25
snmp-server trap 2-25
snmp-server trap community 2-25
snmp-server trap destination 2-25
snmp-server trap heartbeat 2-25
snmp-server trap link-state 2-26
snmp-server trap snmp-authentication 2-26
* snmp-server version 1 2-26
* snmp-server version 2c 2-26
* snmp-server version 3 2-26
snmp-server access interface vlan 2-26
snmp-server access interface gre 2-27
snmp-server access port-2 2-27
snmp-server access lan 2-27
snmp-server access vpn 2-27
snmp-server trap new-satellite-detected 2-27
snmp-server trap satellite-unreachable 2-28
* snmp-server user 2-28
* snmp-server notification receiver 2-28
soap-server 2-28
soap-server access interface vlan 2-28
soap-server access port-1 2-29
soap-server access port-2 2-29
soap-server allow 2-29
soap-server http authentication 2-29
soap-server http authentication password 2-29
soap-server http authentication username 2-30
soap-server port 2-30
soap-server ssl 2-30

soap-server ssl with client certificate 2-30
soap-server access interface gre 2-30
soap-server access lan 2-30
soap-server access vpn 2-31
snmp-server trap vpn-connection 2-31
snmp-server trap syslog-matches 2-31
snmp-server trap syslog-matches regex 2-31
snmp-server trap syslog-severity level 2-31
snmp-server trap network-trace 2-31
firmware-update automatic 2-32
firmware-update start 2-32
firmware-update time 2-32
firmware-update uri 2-32
firmware-update weekday 2-33
snmp-server trap firmware-update 2-33
ip name-server 2-33
ip name-server cache 2-33
ip name-server dynamic 2-33
ip name-server interception 2-34
ip name-server switch-on-servfail 2-34
ip name-server switch-over 2-34
ip name-server logout-info 2-34
access controller shared secret 2-34
radius-server profile 2-35
access controller 2-35
certificate ipsec ca 2-35
certificate ipsec local 2-35
certificate ipsec revocation 2-35
certificate ssl 2-36
session profile default 2-36
session profile 2-36
show session profile 2-36
remote configuration 2-36
discovery protocol 2-36
discovery protocol device-id 2-37
service controller ap authentication credentials 2-37
service controller ap authentication enable 2-37
service controller ap authentication file 2-37
service controller ap authentication radius-server 2-37

service controller ap authentication refresh-rate 2-37
service controller ap authentication source file 2-38
service controller ap authentication source local 2-38
service controller ap authentication source radius 2-38
service controller discovery 2-38
service controller discovery interface internet-port 2-38
service controller discovery interface lan-port 2-38
service controller primary 2-39
service controller primary ip addr 2-39
service controller priority 2-39
service controller provisioning 2-39
bandwidth control internet-port 2-39
bandwidth control internet-port high 2-39
bandwidth control internet-port low 2-40
bandwidth control internet-port max-rate 2-40
bandwidth control internet-port normal 2-41
bandwidth control internet-port very-high 2-41
ip route gateway 2-41
firewall mode 2-41
show user profiles 2-42
show user profiles details 2-42
user profile 2-42
renew user profile subscription 2-42
dot1x reauth 2-42
dot1x reauth period 2-42
dot1x reauth terminate 2-42
dot1x supplicant timeout 2-43
dynamic key 2-43
dynamic key interval 2-43
key chain 2-43
config-version 2-43
radius-server accounting session 2-43
radius-server client 2-44
radius-server local eap-peap 2-44
radius-server local eap-tls 2-44
radius-server local eap-ttls 2-44
radius-server local pap 2-44
radius-server ssid detection nas-id 2-44
show radius-server 2-45

active-directory check attribute 2-45
active-directory check user access 2-45
active-directory device name 2-45
active-directory domain 2-45
active-directory group 2-46
active-directory group order 2-46
active-directory join 2-46
show active-directory 2-46
show active-directory group 2-46
radius-server client 2-46
user tracking 2-46
user tracking destination 2-47
user tracking filter 2-47
user tracking port 2-47
persistent user information 2-47
persistent user information period 2-47
* client data tunnel security 2-47
managed map max 2-47
igmp proxy 2-48
igmp proxy downstream interface 2-48
igmp proxy upstream interface 2-48
* rf-id aeroscout 2-48

Access Controller context 2-49
end 2-49
* ads presentation 2-49
* ads presentation interval 2-49
station allocate source ip address 2-49
station allow any ip address 2-49
station free access 2-50
station http proxy support 2-50
station idle detection 2-50
system accounting 2-51
* remember delay 2-51
* remember html users 2-51
* worldpay installation id 2-51
* worldpay payment response password 2-51
* worldpay payment url 2-51
* authorize_net installation id 2-51
* authorize_net payment url 2-52

* authorize_net transaction key 2-52
* ads presentation with frameset 2-52
authentication http 2-52
authentication https 2-52
noc access internet 2-52
noc access vpn 2-53
noc allow 2-53
noc authentication 2-53
secure login 2-53
* sslv2 authentication 2-53
noc access interface vlan 2-54
noc access interface gre 2-54
ipass id 2-54
ipass name 2-54
wispr abort login url 2-54
wispr login url 2-55
wispr logoff url 2-55
access-list 2-55
use access-list 2-56
use access-list unauth 2-56
config file 2-56
* http proxy upstream 2-57
https ssl certificate 2-57
mac-address 2-57
fail page 2-57
goodbye url 2-57
ipass login url 2-58
login error url 2-58
login page 2-58
login url 2-58
logo 2-58
messages 2-59
noc ssl ca-certificate 2-59
noc ssl certificate 2-59
session page 2-59
transport page 2-59
welcome url 2-60
notify user location changes 2-60

Default Session profile context 2-61
accounting interim update 2-61
idle timeout 2-61
maximum input octets 2-61
maximum input packets 2-61
maximum output octets 2-62
maximum output packets 2-62
maximum total octets 2-62
maximum total packets 2-62
nat one-to-one 2-62
session timeout 2-63
smtp redirection setup 2-63
* public ip subnet 2-63
end 2-63
smtp redirection 2-64

Session profile context 2-65
end 2-65
access controlled 2-65
access list 2-65
accounting interim update 2-65
arp polling interval 2-65
arp polling max count 2-66
bandwidth level 2-66
* egress vlan 2-66
idle timeout 2-66
intercept traffic 2-67
max input rate 2-67
max output rate 2-67
nat one-to-one 2-67
session profile 2-68
smtp redirection setup 2-68
termination action 2-68
user defined attribute 2-69
* public ip subnet 2-69

User Profile context 2-70
end 2-70
access controlled 2-71
access-controlled profile 2-71

access-controlled virtual ap 2-71
active 2-71
chargeable user identity 2-72
control method 2-72
egress vlan 2-72
end time 2-72
idle timeout 2-72
max user sessions 2-72
password 2-73
regular profile 2-73
regular virtual ap 2-73
session timeout 2-73
subscription plan 2-73
username 2-74

Internet interface context 2-75
end 2-75
duplex 2-75
speed 2-75
interface vlan 2-75
ipsec vlan interface 2-76

LAN interface context 2-77
end 2-77
duplex 2-77
speed 2-77
interface vlan 2-77
ipsec vlan interface 2-78

WAN IP interface context 2-79
pppoe client user 2-79
ip address mode 2-79
ip address 2-79
ip nat 2-80
nat limit port range 2-80
nat limit port range size 2-80
ip address dhcp client-id 2-80
end 2-80
pppoe auto-reconnect 2-80
pppoe mru 2-81
pppoe mtu 2-81

pppoe unnumbered 2-81
ip nat outside source static 2-81
ip rip authentication key-chain 2-82
ip rip authentication mode 2-82
ip rip authentication string 2-82
passive-interface 2-82
router rip 2-82
ip address alternate 2-83

LAN IP interface context 2-84
end 2-84
ip address 2-84
ip address management 2-84
passive-interface 2-84
router rip 2-84

RADIUS remote configuration context 2-86
end 2-86
active 2-86
credentials 2-86
interval 2-86
radius server profile 2-86

Virtual AP context 2-87
virtual ap name 2-87
access control 2-87
force centralize data 2-88
ingress interface 2-88
egress unauthenticated 2-88
guest-mode 2-88
max-association 2-89
ssid name 2-89
vlan 2-89
encryption key 1 2-89
encryption key format 2-89
transmit key 2-90
authentication server access controller 2-90
authentication server accounting 2-90
authentication server accounting radius profile 2-90
authentication server radius 2-90
dot1x authentication 2-90

wpa-psk 2-91
authentication server request radius cui 2-91
dot1x session page 2-91
wireless filters 2-91
wireless filters mac 2-92
wireless filters rule input 2-92
wireless filters rule output 2-92
wireless filters type 2-93
mac authentication accounting 2-94
mac authentication accounting radius profile 2-94
mandatory authentication 2-94
mac authentication radius profile 2-94
mac authentication remote 2-94
mac authentication request radius cui 2-94
mac authentication local 2-95
mac authentication 2-95
html authentication 2-95
html authentication accounting 2-95
html authentication accounting radius profile 2-95
html authentication active-directory 2-96
html authentication local 2-96
html authentication radius 2-96
html authentication radius profile 2-96
html authentication request radius cui 2-96
html authentication timeout 2-96
active 2-97
beacon dtim count 2-97
beacon transmit power 2-97
data rate 2-97
public forwarding 2-97
access lan stations 2-97
fast authentication 2-98
layer3 mobility 2-98
add ip-qos profile 2-98
delete ip-qos profile all 2-98
delete ip-qos profile 2-98
qos 2-98
upstream diffserv tagging 2-99
wmm advertising 2-100

html redirection 2-100
local nas id 2-100
bandwidth 2-100
bandwidth default rates 2-100
bandwidth default rates maximum 2-100
radius accounting realms 2-101
radius authentication realms 2-101
identify stations by ip only 2-101
location-aware group 2-101
location-aware called-station-id content 2-101
dhcp relay 2-101
dhcp relay active 2-102
dhcp relay circuit id 2-102
dhcp relay remote id 2-102
dhcp relay subnet 2-102
dhcp server 2-102
dhcp server dns 2-102
dhcp server gateway 2-103
dhcp server range 2-103
dhcp server subnet 2-103
radius-framed-protocol-attribute 2-103
end 2-103
security 2-103

VLAN interface context 2-105
end 2-105
ip address 2-105
ip address mode 2-105
vlan name 2-106
ip default-gateway 2-106
ip nat 2-106

RADIUS context 2-107
end 2-107
radius-server accounting port 2-107
radius-server alternate hosts 2-107
radius-server authentication method 2-107
radius-server authentication port 2-107
radius-server deadtime 2-108
radius-server host 2-108

radius-server key 2 2-108
radius-server message-authenticator 2-108
radius-server name 2-108
radius-server nasid 2-109
radius-server timeout 2-109
radius-server timeout 2-109
radius-server force-nas-port-to-vlanid 2-109
radius-server realm 2-109
radius-server realm name 2-109

DHCP server context 2-110
end 2-110
active 2-110
gateway 2-110
range 2-110
permanent leases 2-110

GRE interface context 2-111
end force 2-111
gre name 2-111
ip address 2-111
peer ip address 2-111
remote ip address 2-111

IPsec policy context 2-112
end 2-112
active 2-112
authentication 2-112
cipher 2-112
dns domain 2-112
dns server 2-112
incoming nat 2-113
incoming traffic network 2-113
interface 2-113
local id 2-113
mode 2-113
outgoing traffic network 2-113
peer id 2-113
peer ip address 2-114
perfect forward secrecy 2-114
preshared key 2-114

Syslog destination context 2-115
active 2-115
logging facility 2-115
logging host 2-115
logging prefix 2-115
name 2-115
end 2-116
level 2-116
level 2-116
matches 2-116
message 2-116
message 2-117
process 2-117
process 2-117

PPTP client interface context 2-118
active 2-118
pptp client credentials 2-118
pptp client domain name 2-118
pptp client server address 2-118
end 2-118
ip nat 2-118
pptp client auto route discovery 2-119
pptp client lcp echo 2-119
passive-interface 2-119
router rip 2-119

Keychain context 2-120
end 2-120
key 2-120
key chain name 2-120

Keys context 2-121
end 2-121
key-string 2-121

Subscription plan context 2-122
end 2-122
daily restriction 2-122
end time 2-122
initial login time allocation 2-122

online time limit 2-123
online time limit 2-123
start time 2-123
subscription plan name 2-123
* public ip reservation 2-123
* public ip subnet 2-123
* SNMP user context 2-125
* access level 2-125
* end 2-125
* password 2-125
* security 2-125
* user name 2-125
* SNMP notification receiver context 2-126
* community 2-126
* end 2-126
* port 2-126
* receiver 2-126
* user 2-126
* version 2-126
Active Directory Group context 2-127
end 2-127
access controlled 2-127
access-controlled profile 2-127
access-controlled virtual ap 2-127
active 2-128
active-directory group name 2-128
egress vlan 2-128
regular profile 2-128
regular virtual ap 2-128
Controlled Network AP context 2-130
end 2-130
execute action 2-130
execute system action 2-130
show config factory 2-130
ap group 2-130
ap name 2-130
config 2-130

contact 2-131
location 2-131
product type 2-131

Controlled Network AP Group context 2-132
execute action 2-132
show config factory 2-132
end 2-132
config 2-132
group name 2-132
virtual ap binding 2-132

Controlled Network Base Group context 2-133
execute action 2-133
show config factory 2-133
config 2-133
end 2-133

Controlled Network context 2-134
end 2-134
* interface wireless 2-134
local mesh group 2-134
local mesh provisioning group 2-134
provisioning connectivity 2-134
provisioning discovery 2-134
radius profile 2-134
* switch port 2-135
syslog 2-135
sensor server name 2-135
sensor server id 2-135
sensor discovery mode 2-135
sensor network detector 2-136
inherit sensor 2-136
dynamic key 2-136
dynamic key interval 2-136
dot1x reauth 2-136
dot1x reauth period 2-137
dot1x reauth terminate 2-137
dot1x supplicant timeout 2-137
inherit 8021x 2-137
bridge protocol ieee 2-137

inherit untagged stp 2-138
bridge protocol ieee vlan 2-138
inherit vlan stp 2-138
inherit local mesh qos 2-138
local mesh ip qos profile 2-138
local mesh qos mechanism 2-139
enable vsc services 2-139
inherit service availability 2-139
inherit l3subnets 2-139
l3subnet 2-139
* inherit switch ports 2-139

Virtual AP Binding context 2-141
dual radio binding 2-141
egress vlan 2-141
egress vlan 2-141
end 2-141
location aware 2-141

Syslog context 2-142
message 2-142
message 2-142
process 2-142
process 2-142
level 2-142
level 2-143
matches 2-143
end 2-143
inherit 2-143

Provisioning connectivity context 2-144
end 2-144
inherit 2-144
interface 2-144
interface provisioninig 2-144
ip assignation 2-144
vlan 2-144
vlan 2-145
static ip 2-145
provisioning local mesh group 2-145
provisioning local mesh key 2-145

provisioning local mesh port....2-145
provisioning local mesh security....2-145
provisioning local mesh security....2-145
provisioning local mesh type....2-146
country code....2-146

Provisioning discovery context....2-147
end....2-147
dns name....2-147
dns provisioning....2-147
inherit....2-147
dns domain name....2-147
dns server....2-148
discovery provisioning....2-148
ip address....2-148
ip provisioning....2-148

CN Wireless interface context....2-149
dot11....2-149
distance....2-149
transmit power....2-150
multicast rate....2-150
dot11 automatic frequency....2-150
dot11 automatic frequency period....2-150
dot11 automatic frequency time....2-150
dot11 automatic transmit-power....2-151
dot11 automatic transmit-power period....2-151
antenna bidirectionnal....2-151
antenna gain....2-151
autochannel skip....2-151
station distance....2-151
beacon interval....2-152
rts threshold....2-152
dot11 mode....2-152
radio active....2-152
spectralink view....2-153
dot11n guard interval....2-153
dot11n channel width....2-153
dot11n channel extension....2-153
dot11n multicast rate....2-153

end 2-153
inherit 2-153

RADIUS Profile context 2-155
end 2-155
inherit 2-155
radius nas id 2-155

Local mesh profile context 2-156
security 2-156
security mode 2-156
security psk 2-156
security wep 2-156
dynamic mode 2-156
mesh id 2-157
allowed downtime 2-157
minimum snr 2-157
snr cost per hop 2-157
initial discovery time 2-157
active 2-157
end 2-157
inherit 2-158
name 2-158
radio active 2-158

Local mesh provisioning profile context 2-159
accept connection 2-159
end 2-159
inherit 2-159
multiple radio 2-159

* Switch port context 2-160
* end 2-160
* active 2-160
* authentication profile vsc 2-160
* authentication server radius 2-160
* dot1x authentication 2-160
* dynamic vlan 2-161
* egress rate 2-161
* force flow control 2-161
* ingress rate 2-161

* ingress traffic type 2-161
* mac authentication 2-162
* mac filter list 2-162
* port name 2-162
* port type 2-162
* power over ethernet 2-162
* priority 2-162
* priority lookup 2-163
* quarantine vlan 2-163
* vlan 2-163

* List of MAC addresses context 2-164
* end 2-164
* entry 2-164
* list name 2-164

Alphabetical list of commands

In this alphabetical list, new to 5.3.x commands are preceded by an asterisk "*" and formatted in green like this:

* command 2-xxx
accept connection 2-159
access control 2-87
access controlled 2-127
access controlled 2-65
access controlled 2-71
access controller 2-35
access controller shared secret 2-34
access lan stations 2-97
* access level 2-125
access list 2-65
access-controlled profile 2-127
access-controlled profile 2-71
access-controlled virtual ap 2-127
access-controlled virtual ap 2-71
access-list 2-55
accounting interim update 2-61
accounting interim update 2-65
active 2-110
active 2-112
active 2-115
active 2-118
active 2-128
active 2-157
* active 2-160
active 2-71
active 2-86
active 2-97
active-directory check attribute 2-45
active-directory check user access 2-45
active-directory device name 2-45
active-directory domain 2-45
active-directory group 2-46
active-directory group name 2-128
active-directory group order 2-46
active-directory join 2-46
add ip-qos profile 2-98
* admin local authentication 2-12
* admin radius authentication 2-12
* admin radius authentication server 2-12
* ads presentation 2-49
* ads presentation interval 2-49
* ads presentation with frameset 2-52
allowed downtime 2-157
antenna bidirectionnal 2-151
antenna gain 2-151
ap group 2-130
ap name 2-130
arp 2-5
arp polling interval 2-65
arp polling max count 2-66
arping 2-2
arping 2-5
authentication 2-112
authentication http 2-52
authentication https 2-52
* authentication profile vsc 2-160
authentication server access controller 2-90
authentication server accounting 2-90
authentication server accounting radius profile 2-90
* authentication server radius 2-160
authentication server radius 2-90
authentication server request radius cui 2-91
* authorize_net installation id 2-51
* authorize_net payment url 2-52
* authorize_net transaction key 2-52
autochannel skip 2-151
bandwidth 2-100
bandwidth control internet-port 2-39
bandwidth control internet-port high 2-39
bandwidth control internet-port low 2-40
bandwidth control internet-port max-rate 2-40
bandwidth control internet-port normal 2-41
bandwidth control internet-port very-high 2-41
bandwidth default rates 2-100
bandwidth default rates maximum 2-100
bandwidth level 2-66
beacon dtim count 2-97
beacon interval 2-152
beacon transmit power 2-97
bridge protocol ieee 2-137
bridge protocol ieee vlan 2-138
certificate 2-9
certificate binding 2-9
certificate ipsec ca 2-35
certificate ipsec local 2-35
certificate ipsec revocation 2-35
certificate revocation 2-9
certificate ssl 2-36
chargeable user identity 2-72
cipher 2-112
* client data tunnel security 2-47
clock 2-18
* clock auto adjust dst 2-19
* clock custom dst begins 2-19
* clock custom dst begins format 2-20
* clock custom dst ends 2-20
* clock custom dst ends format 2-20
clock timezone 2-19
* clock use custom dst rules 2-19
* community 2-126
config 2-130
config 2-132
config 2-133
config 2-7
config file 2-56
config-update automatic 2-21
config-update operation 2-21
config-update time 2-21
config-update uri 2-22
config-update weekday 2-22
config-version 2-43
contact 2-131
control method 2-72
controlled network 2-8
country code 2-146
credentials 2-86
daily restriction 2-122
data rate 2-97
delete ip-qos profile 2-98
delete ip-qos profile all 2-98
dhcp mode 2-16
* dhcp public ip default lease period 2-9

* dhcp public ip subnet 2-9
dhcp relay 2-101
dhcp relay 2-17
dhcp relay access centralized clients 2-18
dhcp relay access lan 2-18
dhcp relay active 2-102
dhcp relay circuit id 2-102
* dhcp relay circuit id 2-17
dhcp relay extend internet port 2-18
dhcp relay remote id 2-102
* dhcp relay remote id 2-18
dhcp relay subnet 2-102
dhcp server 2-102
dhcp server 2-16
dhcp server access centralized clients 2-17
dhcp server access lan 2-17
dhcp server controller 2-16
dhcp server controller discovery 2-16
dhcp server default domain name 2-16
dhcp server default lease period 2-16
dhcp server default permanent lease period 2-16
dhcp server dns 2-102
dhcp server gateway 2-103
dhcp server logout html user 2-17
dhcp server range 2-103
dhcp server subnet 2-103
discovery protocol 2-36
discovery protocol device-id 2-37
discovery provisioning 2-148
distance 2-149
dns domain 2-112
dns domain name 2-147
dns name 2-147
dns provisioning 2-147
dns server 2-112
dns server 2-148
dot11 2-149
dot11 automatic frequency 2-150
dot11 automatic frequency period 2-150
dot11 automatic frequency time 2-150
dot11 automatic transmit-power 2-151
dot11 automatic transmit-power period 2-151
dot11 mode 2-152
dot11n channel extension 2-153
dot11n channel width 2-153
dot11n guard interval 2-153
dot11n multicast rate 2-153
* dot1x authentication 2-160
dot1x authentication 2-90
dot1x reauth 2-136
dot1x reauth 2-42
dot1x reauth period 2-137
dot1x reauth period 2-42
dot1x reauth terminate 2-137
dot1x reauth terminate 2-42
dot1x session page 2-91
dot1x supplicant timeout 2-137
dot1x supplicant timeout 2-43
dual radio binding 2-141
duplex 2-75
duplex 2-77
dynamic key 2-136
dynamic key 2-43
dynamic key interval 2-136
dynamic key interval 2-43
dynamic mode 2-156
* dynamic vlan 2-161
* egress rate 2-161
egress unauthenticated 2-88
egress vlan 2-128
egress vlan 2-141
egress vlan 2-141
* egress vlan 2-66
egress vlan 2-72
enable 2-2
enable vsc services 2-139
encryption key 1 2-89
encryption key format 2-89
end force 2-111
end time 2-122
end time 2-72
* entry 2-164
execute action 2-130
execute action 2-132
execute action 2-133
execute system action 2-130
factory settings 2-10
fail page 2-57
fast authentication 2-98
firewall mode 2-41
firmware-update automatic 2-32
firmware-update start 2-32
firmware-update time 2-32
firmware-update uri 2-32
firmware-update weekday 2-33
force centralize data 2-88
* force flow control 2-161
gateway 2-110
goodbye url 2-57
gre name 2-111
group name 2-132
guest-mode 2-88
html authentication 2-95
html authentication accounting 2-95
html authentication accounting radius profile 2-95
html authentication active-directory 2-96
html authentication local 2-96
html authentication radius 2-96
html authentication radius profile 2-96
html authentication request radius cui 2-96
html authentication timeout 2-96
html redirection 2-100
* http proxy upstream 2-57
https ssl certificate 2-57
identify stations by ip only 2-101
idle timeout 2-61
idle timeout 2-66
idle timeout 2-72
igmp proxy 2-48
igmp proxy downstream interface 2-48
igmp proxy upstream interface 2-48
incoming nat 2-113
incoming traffic network 2-113
ingress interface 2-88
* ingress rate 2-161
* ingress traffic type 2-161
inherit 2-143
inherit 2-144
inherit 2-147
inherit 2-153
inherit 2-155
inherit 2-158

inherit 2-159
inherit 8021x 2-137
inherit l3subnets 2-139
inherit local mesh qos 2-138
inherit sensor 2-136
inherit service availability 2-139
* inherit switch ports 2-139
inherit untagged stp 2-138
inherit vlan stp 2-138
initial discovery time 2-157
initial login time allocation 2-122
intercept traffic 2-67
interface 2-113
interface 2-144
interface ethernet 2-10
interface gre 2-11
interface ip 2-11
interface pptp client-default 2-11
interface provisioninig 2-144
interface vlan 2-75
interface vlan 2-77
* interface wireless 2-134
interval 2-86
ip address 2-105
ip address 2-111
ip address 2-148
ip address 2-79
ip address 2-84
ip address alternate 2-83
ip address dhcp client-id 2-80
ip address management 2-84
ip address mode 2-105
ip address mode 2-79
ip assignation 2-144
ip default-gateway 2-106
ip http port 2-13
ip https port 2-13
ip name-server 2-33
ip name-server cache 2-33
ip name-server dynamic 2-33
ip name-server interception 2-34
ip name-server logout-info 2-34
ip name-server switch-on-servfail 2-34
ip name-server switch-over 2-34
ip nat 2-106
ip nat 2-118
ip nat 2-80
ip nat outside source static 2-81
ip provisioning 2-148
ip rip authentication key-chain 2-82
ip rip authentication mode 2-82
ip rip authentication string 2-82
ip route gateway 2-41
ipass id 2-54
ipass login url 2-58
ipass name 2-54
iperf 2-2
iperf 2-4
ipsec policy 2-12
ipsec vlan interface 2-76
ipsec vlan interface 2-78
key 2-120
key chain 2-43
key chain name 2-120
key-string 2-121
l3subnet 2-139
layer3 mobility 2-98
level 2-116
level 2-116
level 2-142
level 2-143
* list name 2-164
local id 2-113
local mesh group 2-134
local mesh ip qos profile 2-138
local mesh provisioning group 2-134
local mesh qos mechanism 2-139
local nas id 2-100
location 2-131
location aware 2-141
location-aware called-station-id content 2-101
location-aware group 2-101
logging destination 2-22
logging facility 2-115
logging host 2-115
logging prefix 2-115
login error url 2-58
login page 2-58
login url 2-58
logo 2-58
* mac authentication 2-162
mac authentication 2-95
mac authentication accounting 2-94
mac authentication accounting radius profile 2-94
mac authentication local 2-95
mac authentication radius profile 2-94
mac authentication remote 2-94
mac authentication request radius cui 2-94
* mac filter list 2-162
* mac list 2-12
mac-address 2-57
managed map max 2-47
mandatory authentication 2-94
matches 2-116
matches 2-143
max input rate 2-67
max output rate 2-67
max user sessions 2-72
max-association 2-89
maximum input octets 2-61
maximum input packets 2-61
maximum output octets 2-62
maximum output packets 2-62
maximum total octets 2-62
maximum total packets 2-62
mesh id 2-157
message 2-116
message 2-117
message 2-142
message 2-142
messages 2-59
minimum snr 2-157
mode 2-113
multicast rate 2-150
multiple radio 2-159
name 2-115
name 2-158
nat limit port range 2-80
nat limit port range size 2-80
nat one-to-one 2-62
nat one-to-one 2-67
noc access interface gre 2-54

noc access interface vlan 2-54
noc access internet 2-52
noc access vpn 2-53
noc allow 2-53
noc authentication 2-53
noc ssl ca-certificate 2-59
noc ssl certificate 2-59
notify user location changes 2-60
nslookup 2-2
ntp protocol 2-19
ntp server 2-19
ntp server 2-21
ntp server failure trap 2-21
online time limit 2-123
online time limit 2-123
outgoing traffic network 2-113
passive-interface 2-119
passive-interface 2-82
passive-interface 2-84
* password 2-125
password 2-73
peer id 2-113
peer ip address 2-111
peer ip address 2-114
perfect forward secrecy 2-114
permanent leases 2-110
persistent user information 2-47
persistent user information period 2-47
ping 2-2
ping 2-4
* port 2-126
* port name 2-162
* port type 2-162
* power over ethernet 2-162
pppoe auto-reconnect 2-80
pppoe client user 2-79
pppoe mru 2-81
pppoe mtu 2-81
pppoe unnumbered 2-81
pptp client auto route discovery 2-119
pptp client credentials 2-118
pptp client domain name 2-118
pptp client lcp echo 2-119
pptp client server address 2-118
preshared key 2-114
* priority 2-162
* priority lookup 2-163
process 2-117
process 2-117
process 2-142
process 2-142
product type 2-131
provisioning connectivity 2-134
provisioning discovery 2-134
provisioning local mesh group 2-145
provisioning local mesh key 2-145
provisioning local mesh port 2-145
provisioning local mesh security 2-145
provisioning local mesh security 2-145
provisioning local mesh type 2-146
ps 2-3
public forwarding 2-97
* public ip reservation 2-123
* public ip subnet 2-123
* public ip subnet 2-63
* public ip subnet 2-69
qos 2-98
* quarantine vlan 2-163
quit 2-3
quit 2-5
radio active 2-152
radio active 2-158
radius accounting realms 2-101
radius authentication realms 2-101
radius nas id 2-155
radius profile 2-134
radius server profile 2-86
radius-framed-protocol-attribute 2-103
radius-server accounting port 2-107
radius-server accounting session 2-43
radius-server alternate hosts 2-107
radius-server authentication method 2-107
radius-server authentication port 2-107
radius-server client 2-44
radius-server client 2-46
radius-server deadtime 2-108
radius-server force-nas-port-to-vlanid 2-109
radius-server host 2-108
radius-server key 2 2-108
radius-server local eap-peap 2-44
radius-server local eap-tls 2-44
radius-server local eap-ttls 2-44
radius-server local pap 2-44
radius-server message-authenticator 2-108
radius-server name 2-108
radius-server nasid 2-109
radius-server profile 2-35
radius-server realm 2-109
radius-server realm name 2-109
radius-server ssid detection nas-id 2-44
radius-server timeout 2-109
radius-server timeout 2-109
range 2-110
rcapture 2-5
reboot device 2-10
reboot device 2-4
* receiver 2-126
regular profile 2-128
regular profile 2-73
regular virtual ap 2-128
regular virtual ap 2-73
* remember delay 2-51
* remember html users 2-51
remote configuration 2-36
remote ip address 2-111
renew user profile subscription 2-42
* rf-id aeroscout 2-48
router rip 2-119
router rip 2-82
router rip 2-84
rts threshold 2-152
secure login 2-53
security 2-103
* security 2-125
security 2-156
security mode 2-156
security psk 2-156
security wep 2-156
sensor discovery mode 2-135
sensor network detector 2-136
sensor server id 2-135
sensor server name 2-135

service controller ap authentication credentials 2-37
service controller ap authentication enable 2-37
service controller ap authentication file 2-37
service controller ap authentication radius-server 2-37
service controller ap authentication refresh-rate 2-37
service controller ap authentication source file 2-38
service controller ap authentication source local 2-38
service controller ap authentication source radius 2-38
service controller discovery 2-38
service controller discovery interface internet-port 2-38
service controller discovery interface lan-port 2-38
service controller primary 2-39
service controller primary ip addr 2-39
service controller priority 2-39
service controller provisioning 2-39
session page 2-59
session profile 2-36
session profile 2-68
session profile default 2-36
session timeout 2-63
session timeout 2-73
show active-directory 2-46
show active-directory group 2-46
show all config 2-7
show arp 2-5
show bridge 2-5
show bridge forwarding 2-6
show certificate 2-10
show certificate 2-4
show certificate binding 2-10
show certificate binding 2-4
show client log 2-7
show config factory 2-10
show config factory 2-130
show config factory 2-132
show config factory 2-133
show controlled network config 2-8
show discrete pin 2-7
show dns cache 2-6
show interfaces 2-6
* show ip 2-6
show ip dhcp database 2-6
show ip route 2-6
show license 2-3
show logging filtered 2-3
* show mac list 2-12
show radius statistics 2-7
show radius users 2-7
show radius-server 2-45
show satellites 2-6
show session profile 2-36
show subscription plan 2-11
show system info 2-6
show user profiles 2-42
show user profiles details 2-42
show users 2-7
* show web content 2-7
smtp redirection 2-64
smtp redirection setup 2-63
smtp redirection setup 2-68
snmp-server 2-23
snmp-server access interface gre 2-27
snmp-server access interface vlan 2-26
snmp-server access lan 2-27
snmp-server access port-1 2-23
snmp-server access port-2 2-27
snmp-server access vpn 2-27
snmp-server allow 2-23
snmp-server chassis-id 2-23
snmp-server contact 2-24
snmp-server heartbeat period 2-24
snmp-server location 2-24
* snmp-server notification receiver 2-28
snmp-server port 2-24
snmp-server readonly 2-24
snmp-server readwrite 2-25
snmp-server trap 2-25
snmp-server trap certificate-expired 2-13
snmp-server trap certificate-expires-soon 2-13
snmp-server trap community 2-25
snmp-server trap config-change 2-22
snmp-server trap config-update 2-22
snmp-server trap destination 2-25
snmp-server trap firmware-update 2-33
snmp-server trap heartbeat 2-25
snmp-server trap link-state 2-26
snmp-server trap network-trace 2-31
snmp-server trap new-satellite-detected 2-27
snmp-server trap satellite-unreachable 2-28
snmp-server trap snmp-authentication 2-26
snmp-server trap syslog-matches 2-31
snmp-server trap syslog-matches regex 2-31
snmp-server trap syslog-severity 2-23
snmp-server trap syslog-severity level 2-31
snmp-server trap vpn-connection 2-31
snmp-server trap web-fail 2-13
snmp-server trap web-login 2-14
snmp-server trap web-logout 2-14
* snmp-server user 2-28
* snmp-server version 1 2-26
* snmp-server version 2c 2-26
* snmp-server version 3 2-26
snr cost per hop 2-157
soap-server 2-28
soap-server access interface gre 2-30
soap-server access interface vlan 2-28
soap-server access lan 2-30
soap-server access port-1 2-29
soap-server access port-2 2-29
soap-server access vpn 2-31
soap-server allow 2-29
soap-server http authentication 2-29
soap-server http authentication password 2-29
soap-server http authentication username 2-30
soap-server port 2-30
soap-server ssl 2-30
soap-server ssl with client certificate 2-30
spectralink view 2-153
speed 2-75
speed 2-77
ssid name 2-89
* sslv2 authentication 2-53
start time 2-123
static ip 2-145
station allocate source ip address 2-49
station allow any ip address 2-49
station distance 2-151
station free access 2-50
station http proxy support 2-50
station idle detection 2-50
subscription plan 2-11
subscription plan 2-73

subscription plan name 2-123
* switch port 2-135
syslog 2-135
system accounting 2-51
termination action 2-68
top 2-3
traceroute 2-3
transmit key 2-90
transmit power 2-150
transport page 2-59
upstream diffserv tagging 2-99
use access-list 2-56
use access-list unauth 2-56
* user 2-126
user defined attribute 2-69
* user name 2-125
user profile 2-42
user tracking 2-46
user tracking destination 2-47
user tracking filter 2-47
user tracking port 2-47
username 2-10
username 2-74
* version 2-126
virtual ap 2-11
virtual ap binding 2-132
virtual ap name 2-87
vlan 2-144
vlan 2-145
* vlan 2-163
vlan 2-89
vlan name 2-106
web access interface gre 2-15
web access interface vlan 2-15
web access internet-port 2-15
web access lan 2-15
web access lan-port 2-15
web access vpn 2-15
web admin kickout 2-14
web allow 2-14
welcome url 2-60
wireless filters 2-91
wireless filters mac 2-92
wireless filters rule input 2-92
wireless filters rule output 2-92
wireless filters type 2-93
wispr abort login url 2-54
wispr login url 2-55
wispr logoff url 2-55
wmm advertising 2-100
world-mode dot11 country code 2-14
* worldpay installation id 2-51
* worldpay payment response password 2-51
* worldpay payment url 2-51
wpa-psk 2-91

1

Introduction

Contents

About this guide 1-2
- Products covered 1-2
- HP ProCurve Product Naming 1-2
- Important terms 1-3
- Typographical conventions 1-3

HP ProCurve Networking support 1-4

Online documentation 1-5

Configuring CLI support 1-5
- SSH client support 1-6

Entering strings 1-6

Context hierarchy 1-7

Sample CLI session 1-8

File transfer 1-8

About this guide

This guide explains how to work with the Command Line Interface (CLI) on HP ProCurve Networking MSM7xx Controllers.

Products covered

This guide covers the following products:

Model	Part
MSM710 Access Controller	J9328A
MSM710 Mobility Controller	J9325A
MSM730 Access Controller	J9329A
MSM730 Mobility Controller	J9326A
MSM750 Access Controller	J9330A
MSM750 Mobility Controller	J9327A
MSM760 Access Controller	J9420A
MSM760 Mobility Controller	J9421A
MSM765 Mobility Controller	J9370A

HP ProCurve Product Naming

As of October 1st, 2008, Colubris Networks was acquired by HP ProCurve. HP ProCurve has begun integrating the Colubris product line into the HP ProCurve Networking product portfolio (www.procurve.com/news/colubris-10-01-08.htm).

In the online help and this manual, Colubris product names have been changed to their equivalent HP ProCurve product names.

Note

SOAP and SNMP MIBs retain the Colubris naming so you do not need to change your existing SOAP and MIB usage.

The Colubris Networks product names and their corresponding new HP ProCurve product names are as follows:

Colubris name	HP ProCurve name
MSC-5100 MultiService Controller	MSM710 Controller
MSC-5200 MultiService Controller	MSM730 Controller
MSC-5500 MultiService Controller	MSM750 Controller
MAP-320 MultiService Access Point	MSM310 Access Point

Colubris name	HP ProCurve name
MAP-320R MultiService Access Point	MSM310-R Access Point
MAP-330 MultiService Access Point	MSM320 Access Point
MAP-330R MultiService Access Point	MSM320-R Access Point
MAP-330 AP+Sensor MultiService Access Point	MSM325 Access Point with Sensor
MAP-625 MultiService Access Point	MSM422 Access Point
MAP-630 AP+Sensor MultiService Access Point	MSM335 Access Point with Sensor
WCB-200 Wireless Client Bridge	M111 Client Bridge
Visitor Management Tool	Guest Management Software
RF Manager 1500 Enterprise	RF Manager 100 IDS/IPS system
RF Manager 1300 Basic	RF Manager 50 IDS/IPS system
RF Planner	RF Planner

Important terms

The following terms are used in this guide.

Term	Description
AP	Refers to any HP ProCurve Networking MSM3xx or MSM4xx Access Point.
service controller	Refers to any HP ProCurve Networking MSM7xx Controller, including both Access Controller and Mobility Controller variants.
VSC, Virtual ap, VAP	These terms are used interchangeably to refer to VSC (Virtual Service Community).

Typographical conventions

Command syntax

Command syntax is formatted in a monospaced font as follows:

Example	Description
`web admin kickout`	Items in plain text must be entered as shown.
`ip http port <number>`	Items in italics and enclosed in < > are parameters for which you must supply a value. In this example, you must supply a value for <*number*>.

Example	Description
`end [force]`	Items enclosed in square brackets are optional. You can either include them or not. Do not include the brackets. In this example you can either include “force” or omit it.
`firewall mode (high|low|none)`	Items enclosed in parenthesis and separated by a vertical line indicate a choice. Specify only one of the items. In this example, you must specify ’high’, ’low’, or ’none’.

Management tool

When referring to the management tool interface, the Main menu name is presented first followed by a right angle-bracket and then the sub-menu name, as in **Network > Ports**.

Double angle brackets **>>** separate elements that appear in the Network Tree from main menu and sub-menu references, as in **Service Controller >> Status**.

HP ProCurve Networking support

HP ProCurve Networking offers support 24 hours a day, seven days a week through a number of automated electronic services. See the Customer Support/Warranty booklet included with your product.

The HP ProCurve Networking Web site, **www.procurve.com/customercare** provides up-to-date support information.

Additionally, your HP-authorized network reseller can provide you with assistance, both with services that they offer and with services offered by HP.

Before contacting support

To make the support process most efficient, before calling your networking dealer or HP Support, you first should collect the following information:

Collect this information	Where to find it
Product identification.	On the rear of the product.
Software version.	The service controller management tool **Login** page.
Network topology map, including the addresses assigned to all relevant devices.	Your network administrator.

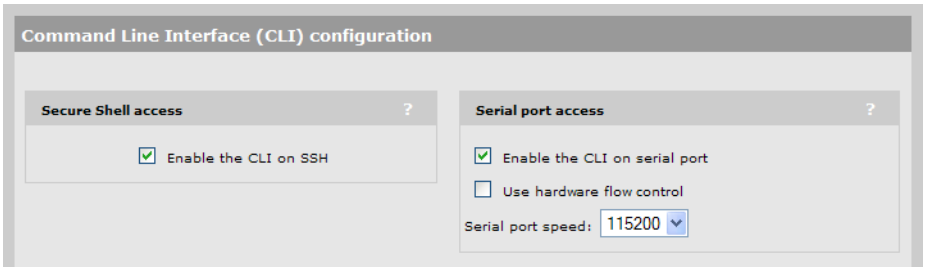
Online documentation

For the latest documentation, visit the HP ProCurve Networking manuals Web page at: **www.procurve.com/manuals**.

Configuring CLI support

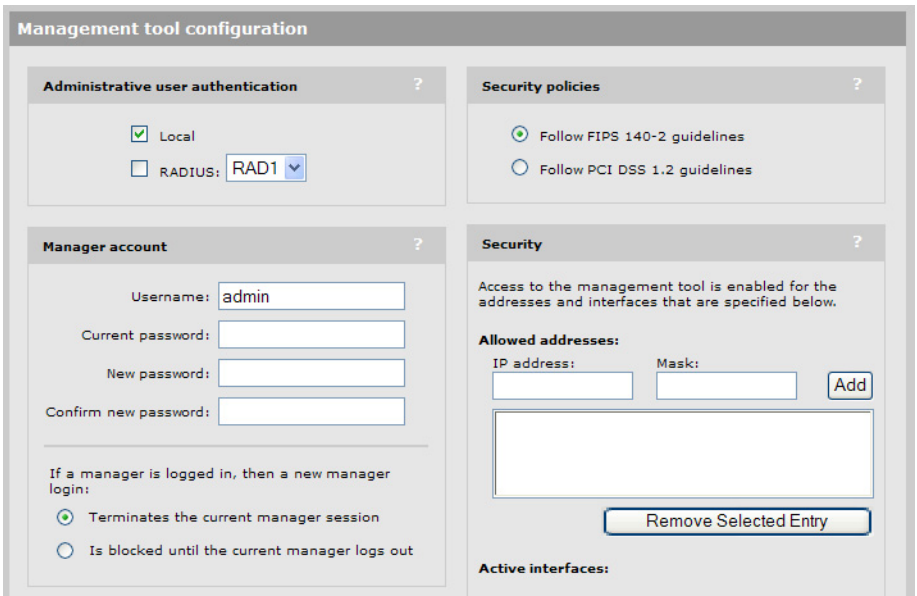
Using the service controller management tool, open the CLI configuration page. Select **Service controller >> Management > CLI**.

Use this page to enable/disable CLI support via an SSH or serial connection. A maximum of three concurrent CLI sessions are supported regardless of the connection type.



The CLI supports SSH on the standard TCP port (22).

Connectivity and login credentials for SSH connections use the same settings as defined for the management tool manager on the **Service Controller >> Management > Management tool** page.



- SSH connections to the CLI can be made on any active interface. Support for each interface must be explicitly enabled under **Security.**
- The login credentials for SSH connections are the same as those defined under **Manager account**. By default, both username and password are set to **admin**.

Note

SSH logins always use the local manager username and password, even if **Administrative user authentication** is set to use a RADIUS server. (The **Administrative user authentication** option is not available on all models.)

SSH client support

The following SSH clients have been tested with the CLI. Others may work as well:

- OpenSSH
- Tectia
- SecureCRT
- Putty

Entering strings

When entering a value that contains spaces, you must enclose it in quotation marks. For example, if the command syntax is:

```
ssid <name>
```

You must specify one of the following:

```
ssid ANameWithNoSpaces
ssid "A name with spaces"
```

Context hierarchy

CLI commands are grouped into functional contexts. The following table show the context hierarchy and the command used to switch from the parent context:

Context hierarchy	Command to switch from parent context
View context	*(This is the first context. No command is needed.)*
Enable context	enable
Config context	config
WAN IP interface context	interface ip wan
LAN IP interface context	interface ip lan
Internet interface context	interface ethernet port-2
VLAN interface context	interface vlan <*id*>[-<*id2*>]
LAN interface context	interface ethernet port-1
VLAN interface context	interface vlan <*id*>[-<*id2*>]
PPTP client interface	interface pptp client-default
GRE interface context	interface gre <*name*>
Virtual AP context	virtual ap <*name*>
Subscription plan	subscription plan <*name*>
List of MAC addresses context	mac list <*name*>
IPsec policy context	ipsec policy <*name*>
DHCP server context	dhcp server lan
Syslog destination context	logging destination <*name*>
SNMP user context	snmp-server user <*name*>
SNMP notification receiver context	snmp-server notification receiver <*host*>
RADIUS context	radius-server profile <*name*>
Access Controller context	access controller
Default Session profile context	session profile default
Session profile context	session profile <*name*>
RADIUS remote configuration context	remote configuration radius
User Profile context	user profile <*name*>
Keychain context	key chain <*name*>
Keys context	key <*number*>
Active Directory Group context	active-directory group <*name*>
Controlled Network AP context	controlled network (ap <*name*> [<*mac*>]
Controlled Network context	config
CN Wireless interface context	interface wireless (single|dual|triple) <*number*>
RADIUS Profile context	radius profile <*profile*>
Local mesh profile context	local mesh group <*group*>
Local mesh provisioning profile context	local mesh provisioning group
Provisioning connectivity context	provisioning connectivity
Provisioning discovery context	provisioning discovery
Syslog context	syslog
Switch port context	switch port <*name*>
Controlled Network AP Group context	controlled network (group <*name*> [<*mac*>]
Virtual AP Binding context	virtual ap binding <*profile*>
Controlled Network context	config
CN Wireless interface context	interface wireless (single|dual|triple) <*number*>
RADIUS Profile context	radius profile <*profile*>
Local mesh profile context	local mesh group <*group*>
Local mesh provisioning profile context	local mesh provisioning group
Provisioning connectivity context	provisioning connectivity
Provisioning discovery context	provisioning discovery
Syslog context	syslog
Switch port context	switch port <*name*>
Controlled Network Base Group context	controlled network base
Controlled Network context	config
CN Wireless interface context	interface wireless (single|dual|triple) <*number*>
RADIUS Profile context	radius profile <*profile*>
Local mesh profile context	local mesh group <*group*>
Local mesh provisioning profile context	local mesh provisioning group
Provisioning connectivity context	provisioning connectivity
Provisioning discovery context	provisioning discovery
Syslog context	syslog
Switch port context	switch port <*name*>

Sample CLI session

This sample CLI session shows you how to set the WAN port to use a static IP address, disable NAT, and add an alternate IP address. (The CLI prompt is shown in bold.)

```
CLI> enable
CLI# config
CLI(config)# interface ip wan
CLI(config-if-ip)# ip address 192.168.66.1/24
CLI(config-if-ip)# ip address mode static
CLI(config-if-ip)# no ip nat
CLI(config-if-ip)# ip address alternate 192.168.23.56
CLI(config-if-ip)# end
CLI(config)# end
CLI# quit
```

File transfer

In some cases you may need to transfer files (certificates or configuration) to the service controller. Commands that have this capability typically include <uri> or <url> in their parameter list.

Note

When you enter the commands discussed here, the files are transferred immediately.

File transfer can be performed in two ways.

A. The service controller gets the file using a URL

Transfer a certificate file using ftp. For example:

```
certificate ipsec ca ftp://ftp.example.com/certificate/my-root-certificate.pem
```

B. Send a file to the service controller

Using SFTP (available with OpenSSH or SSH), authenticate with the CLI credentials. Then send the file to the service controller. For example:

```
sftp msm710.mycompany.com
>login: admin
>password: ****
>put my-root-certificate.pem
file transferred (1k)
>quit
```

In the CLI, use the local://<*filename*> parameter in the URL. Replace <*filename*> with the filename you used to transfer using SFTP. For example:

```
CLI(config)# certificate ipsec ca local://my-root-certificate.pem
```

2

CLI commands

View context

Path: View

This is the root of the command tree.

arping

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`arping [ -AbDfhqUV] [ -c <count>] [ -w <deadline>] [ -s <source>] -I <interface> <destination>`

Pings a destination on a device interface using ARP packets.

enable

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`enable`

Switches to the enable context.

iperf

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`iperf -c host [-t time]`

Runs a performance throughput test.

Parameters

<-c host>	The IP address or DNS name of the iperf server to connect to.
<-t length>	Length of the throughput test in seconds.

nslookup

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`nslookup [ -option authentication ] [ <host-to-find> | - [< server> ]]`

Queries DNS servers for information on hosts or domains.

ping

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`ping <host> [-c <count>] [-s <length>] [-q]`

Determines if the specified remote IP address is active.

Parameters

<-c host>	The IP address or DNS name of the host to ping.
<-c count>	Number of pings.
<-s length>	Length of the ping datagram.
<-q>	Quiet mode. No output.

ps

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
ps
```

Displays all running processes.

quit

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
quit
```

Quits the CLI.

show license

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
show license (eula | gpl | other)
```

Displays license information.

show logging filtered

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
show logging [filtered]
```

Displays the system log.

top

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
top
```

Displays all running processes.

traceroute

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
traceroute [-n] [-r] [-v] [-m <max_ttl>] [-p <port#>] [-q <nqueries>] [-s
<src_addr>] [-t <tos>] [-w <wait>] <host> [<data size>]
```

Show the hosts that are traversed to reach the specified IP address.

Enable context

Path: View > Enable

This context provides access to various utilities.

reboot device

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
reboot device
```

Restarts the system.

show certificate

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
show certificate
```

Display current certificates.

show certificate binding

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
show certificate binding
```

Display how the certificates are used.

iperf

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
iperf -c host [-t time]
```

Runs a performance throughput test.

Parameters

<-c host>	The IP address or DNS name of the iperf server to connect to.
<-t length>	Length of the throughput test in seconds.

ping

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
ping <host> [-c <count>] [-s <length>] [-q]
```

Determines if the specified remote IP address is active.

Parameters

<-c host>	The IP address or DNS name of the host to ping.
<-c count>	Number of pings.
<-s length>	Length of the ping datagram.
<-q>	Quiet mode. No output.

arping

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`arping [ -AbDfhqUV] [ -c <count>] [ -w <deadline>] [ -s <source>] -I <interface> <destination>`

Pings a destination on a device interface using ARP packets.

arp

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`arp [-evn] [-H <type>] [-i if] ?- [<hostname>] arp [-v] [-i if] -d <hostname> [pub] arp [-v] [-H <type>] [-i if] -s <hostname> <hw_addr> [temp] arp [-v] [-H <type>] [-i if] -s <hostname> <hw_addr> [<netmask> <nm>] <pub> arp [-v] [-H <type>] [-i if] -Ds <hostname> ifa [<netmask> <nm>] <pub>`

Displays and modifies the Internet-to-Ethernet address translation tables used by the address resolution protocol.

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`end`

Switches to parent context.

quit

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`quit`

Exit the enable context.

rcapture

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`rcapture [<a>] [<b>] [<c>] [<d>] [<e>] [<f>] [<g>] [<h>]`

Sends port capture to an FTP server.

Refer to Linux documentation for a complete description of this command and its options.

show arp

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`show arp`

Show the ARP table.

show bridge

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`show bridge`

Show bridge information.

show bridge forwarding

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`show bridge forwarding`

Show bridge forwarding information.

show dns cache

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`show dns cache [<serial>]`

Show DNS cache entries. Specify a serial number to display detailed information.

show interfaces

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`show interfaces`

Show networking interfaces.

show ip

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`show ip`

Show all IP addresses, mask, MTU, and MAC addresses.

show ip route

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`show ip route`

Show all IP routes.

show system info

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`show system info`

Show basic system information.

show ip dhcp database

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`show ip dhcp database`

Show the DHCP server lease database.

show satellites

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`show satellites [<deviceid>]`

Show current satellites of this access point.

show web content

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`show web content`

Show all files inside the access points detected nearby.

show client log

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`show client log [<macaddr>]`

Display client station log. Enter the MAC address to display more details for a specific client station.

show radius statistics

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`show radius statistics`

Show RADIUS server statistics.

show radius users

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`show radius users [<filter>]`

Show users that are using RADIUS accounting.

show users

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`show users [<filter>]`

Show all users of this service controller.

show discrete pin

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`show discrete pin`

Display the state of the discrete pin.

config

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`config`

Switches to the config context.

show all config

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`show all config`

Print all configuration that applies to this device.

controlled network

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`controlled network (ap | group | base) [<name>] [<mac>]`

Create/use the controlled network entity.

show controlled network config

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`show controlled network config`

Print configuration for all Controlled Network entities.

Config context

Path: View > Enable > Config

This is the root context for all configuration commands.

dhcp public ip default lease period

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`dhcp public ip default lease period <number>`

Sets the default lease time for the DHCP public IP subnet pool.

dhcp public ip subnet

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`dhcp public ip subnet`

Enable DHCP server IP Address pool for Access Controller public IP subnet functionality.

`no dhcp public ip subnet`

Disable DHCP server IP Address pool for Access Controller public IP subnet functionality.

certificate

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`certificate (authority | local) <uri> <certname> [<password>]`

Add a new certificate to the store, using the friendly name.

certificate binding

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`certificate binding (web-management | html-auth | soap | eap) <certname>`

Assign a certificate to a service.

`no certificate binding (web-management | html-auth | soap | eap) <certname>`

Unassign a certificate from a service.

certificate revocation

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`certificate revocation <uri> <certname>`

Add a Certificate Revocation List to an existing authority certificate.

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`end`

Switches to parent context.

factory settings

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
factory settings
```

Resets the system configuration to factory default settings.

interface ethernet

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
interface ethernet (port-1|port-2)
```

Switches to the specified Ethernet interface context.

reboot device

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
reboot device
```

Restarts the system.

show certificate

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
show certificate
```

Display current certificates.

show certificate binding

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
show certificate binding
```

Display how the certificates are used.

show config factory

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
show config [factory]
```

Generates a list of CLI commands that can be used to define the currently loaded configuration.

username

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
username <user> <password>
```

Changes the current administrator username and password.

Parameters

<user>	New administrator username.
<password>	New administrator password.

interface ip

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`interface ip (lan | wan)`

Switches to the specified IP interface context.

interface pptp client-default

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`interface pptp client-default`

Switches to the PPTP client interface context.

interface gre

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`interface gre <name>`

Switches to the specified GRE interface or creates a new GRE interface with the specified name.

`no interface gre <name>`

Deletes the specified GRE interface.

virtual ap

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`virtual ap <name>`

Creates a new VAP (VSC) profile or switches to the existing VAP (VSC) context with the specified name.

`no virtual ap <name>`

Deletes the specified Virtual AP profile.

Parameters

`name`	Name of an existing or new VAP (VSC) profile.

show subscription plan

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`show subscription plan [<name>]`

Display one or many subscription plans.

subscription plan

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`subscription plan <name>`

Add a new subscription plan.

`no subscription plan <name>`

Delete a subscription plan.

mac list

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`mac list <name>`

Edit a MAC list.

`no mac list <name>`

Delete a MAC list by name.

show mac list

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`show mac list [<name>]`

Display current MAC list, or one list in detail.

ipsec policy

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`ipsec policy <name>`

Switches to the specified IPSec policy or creates a new IPSec policy with the specified name.

admin local authentication

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`admin local authentication`

Enable the authentication of administrator logins to occur using local account.

`no admin local authentication`

Disable administrator authentication via local account.

admin radius authentication

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`admin radius authentication`

Sets the authentication of administrator logins to occur using RADIUS.

`no admin radius authentication`

Disable administrator authentication via RADIUS.

admin radius authentication server

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`admin radius authentication server <name>`

Sets the authentication of administrator logins to occur using RADIUS.

ip http port

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`ip http port <number>`

Sets the port number to use for HTTP access to the service controller.

Parameters

<number> Port number. Range: 1 - 65535.

Description

HTTP connections made to this port are met with a warning and the browser is redirected to the secure web server port. By default. this parameter is set to port 80.

ip https port

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`ip https port <number>`

Sets the port number used for HTTPS access to the service controller.

Parameters

<number> Port number. Range: 1 - 65535.

snmp-server trap certificate-expired

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`snmp-server trap certificate-expired`

Send a trap when the SSL certificate has expired. A trap is sent every 12 hours.

`no snmp-server trap certificate-expired`

Do not send a trap when the SSL certificate has expired.

snmp-server trap certificate-expires-soon

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`snmp-server trap certificate-expires-soon`

Send a trap when the SSL certificate is about to expire. A trap is sent every 12 hours starting 15 days before the certificate expires.

`no snmp-server trap certificate-expires-soon`

Do not send a trap when the SSL certificate is about to expire.

snmp-server trap web-fail

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`snmp-server trap web-fail`

Send a trap each time an administrator login is refused.

`no snmp-server trap web-fail`

Do not send a trap each time an administrator login is refused.

snmp-server trap web-login

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`snmp-server trap web-login`

Send a trap each time an administrator login is accepted.

`no snmp-server trap web-login`

Do not send a trap each time an administrator login is accepted.

snmp-server trap web-logout

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`snmp-server trap web-logout`

Send a trap each time an administrator logs out.

`no snmp-server trap web-logout`

Do not send a trap each time an administrator logs out.

web admin kickout

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`web admin kickout`

Enables a new administrator login to terminate an existing administrator session.

`no web admin kickout`

Stops a new administrator from logging in until an existing administrator logs out.

web allow

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`web allow <ip address>/<mask>`

Adds an address to the list of hosts that can access the management tool.

`no web allow <ip address>/<mask>`

Removes the specified address from the list of hosts that can access the management tool.

Parameters

<address>	IP address.
</mask>	Subnet mask in CIDR format. Specifies the number of bits in the mask.

world-mode dot11 country code

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`world-mode dot11 country code <code>`

Specifies the country the service controller is operating in.

Parameters

<code>	An ISO3166 three-letter country code.

web access internet-port

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
web access internet-port
```

Enables access to the management tool via the Internet port.

```
no web access internet-port
```

Blocks access to the management tool via the Internet port.

web access lan-port

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
web access lan-port
```

Enables access to the management tool via the LAN port.

```
no web access lan-port
```

Blocks access to the management tool via the LAN port.

web access interface vlan

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
web access interface vlan <name>
```

Enables access to the management tool via the specified VLAN.

```
no web access interface vlan <name>
```

Removes access to the management tool for the specified VLAN.

web access interface gre

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
web access interface gre <name>
```

Enables access to the management tool via the specified GRE tunnel.

```
no web access interface gre <name>
```

Disables access to the management tool via the specified GRE tunnel.

web access lan

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
web access lan
```

Enables access to the management tool via the LAN port.

```
no web access lan
```

Blocks access to the management tool via the LAN port.

web access vpn

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
web access vpn
```

Enables access to the management tool via a VPN connection.

`no web access vpn`

Blocks access to the management tool via a VPN connection.

dhcp mode

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`dhcp mode (server | relay | none)`

Sets whether the service controller operates as a DHCP server or DHCP relay agent.

dhcp server

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`dhcp server lan`

Switches to the DHCP server context.

dhcp server default domain name

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`dhcp server default domain name <domain>`

Sets the DHCP server domain name.

dhcp server default lease period

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`dhcp server default lease period <number>`

Sets the default lease time for the DHCP server.

dhcp server default permanent lease period

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`dhcp server default permanent lease period <number>`

Sets the permanent lease time for the DHCP server.

dhcp server controller

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`dhcp server controller <ip address>`

Add the IP address to the list of controllers.

`no dhcp server controller <ip address>`

Remove the IP address from the list of controllers.

dhcp server controller discovery

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`dhcp server controller discovery`

Send the list of controller IP addresses with DHCP answers.

```
no dhcp server controller discovery
```

Do not send the list of controller IP addresses with DHCP answers.

dhcp server logout html user

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
dhcp server logout html user
```

Logout HTML user upon discover request.

```
no dhcp server logout html user
```

Do not logout HTML user upon discover request.

dhcp server access centralized clients

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
dhcp server access centralized clients
```

Listen for DHCP requests from centralized access-controlled client stations.

```
no dhcp server access centralized clients
```

Do not listen for DHCP requests from centralized access-controlled client stations.

dhcp server access lan

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
dhcp server access lan
```

Listen for DHCP requests on the LAN interface.

```
no dhcp server access lan
```

Do not listen for DHCP requests on the LAN interface.

dhcp relay

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
dhcp relay <primary-ip-address> <[secondary-ip-address]>
```

Sets the primary and secondary DHCP server for the relay.

dhcp relay circuit id

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
dhcp relay circuit id <string>
```

Sets the Option 82 circuit ID.

```
no dhcp relay circuit id
```

Clears the Option 82 circuit ID.

dhcp relay remote id

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`dhcp relay remote id <string>`

Sets the Option 82 remote ID.

`no dhcp relay remote id`

Clears the Option 82 remote ID.

dhcp relay access centralized clients

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`dhcp relay access centralized clients`

Listen for DHCP requests from centralized access-controlled client stations.

`no dhcp relay access centralized clients`

Do not listen for DHCP requests from centralized access-controlled client stations.

dhcp relay access lan

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`dhcp relay access lan`

Listen for DHCP requests on the LAN interface.

`no dhcp relay access lan`

Do not listen for DHCP requests on the LAN interface.

dhcp relay extend internet port

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`dhcp relay extend internet port`

Alter DHCP requests so they appear from the Internet port.

`no dhcp relay extend internet port`

Do not alter DHCP requests.

clock

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`clock <time> <date>`

Sets the system time and date.

Parameters

<time>	Time as hh:mm:ss. For example: 15:44:00.
<date>	Date as dd Month yyyy. For example: 17 Oct 2004.

clock auto adjust dst

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`clock auto adjust dst`

Automatically adjust clock for daylight savings changes.

`no clock auto adjust dst`

Do not automatically adjust clock for daylight savings changes.

clock timezone

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`clock timezone <gmtdiff>`

Sets the time zone the service controller is operating in.

Parameters

<gmtdiff>	Offset from GMT as follows: +-HOUR:MIN. For example, Eastern Standard time is -5:00.

clock use custom dst rules

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`clock use custom dst rules`

Use custom DST rules instead of default ones.

`no clock use custom dst rules`

Do not use custom DST rules, use default ones.

ntp protocol

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`ntp protocol (ntp | sntp)`

Sets the network time protocol to use.

ntp server

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`ntp server`

Enable this option to have the service controller periodically contact a network time server to update its internal clock.

`no ntp server`

Disables the use of a network time server.

clock custom dst begins

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`clock custom dst begins <day> <weekday> <month> <time>`

Set parameters of the rule defining the beginning of daylight savings time.

Parameters

<day>	Day of the month. Range 1 - 31.
<weekday>	Weekday. Valid values are: "sun", "mon", "tue", "wed", "thu", "fri", "sat".
<month>	Month. Valid values are: "jan", "feb", "mar", "apr", "may", "jun", "jul", "aug", "sep", "oct", "nov", "dec".
<time>	Time as hh:mm[:ss]. For example: 15:44:00.

If a parameter does not apply to the configured DST rule format, simply set this parameter to any valid value.

clock custom dst begins format

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
clock custom dst begins format (fixed | last-weekday | following-date | preceding-date)
```

Set the format of the custom DST rule.

Parameters

<fixed>	Rule of the form: The [Day]th of [Month] at [Time].
<last-weekday>	Rule of the form: The last [Weekday] of [Month] at [Time].
<following-date>	Rule of the form: The first [Weekday] on or after the [Day]th of [Month] at [Time].
<preceding-date>	Rule of the form: The first [Weekday] on or before the [Day]th of [Month] at [Time].

clock custom dst ends

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
clock custom dst end <day> <weekday> <month> <time>
```

Set parameters of the rule defining the end of daylight savings time.

Parameters

<day>	Day of the month. Range 1 - 31.
<weekday>	Weekday. Valid values are: "sun", "mon", "tue", "wed", "thu", "fri", "sat".
<month>	Month. Valid values are: "jan", "feb", "mar", "apr", "may", "jun", "jul", "aug", "sep", "oct", "nov", "dec".
<time>	Time as hh:mm[:ss]. For example: 15:44:00.

If a parameter does not apply to the configured DST rule format, simply set this parameter to any valid value.

clock custom dst ends format

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
clock custom dst ends format (fixed | last-weekday | following-date | preceding-date)
```

Set the format of the custom DST rule.

Parameters

<fixed>	Rule of the form: The [Day]th of [Month] at [Time].
<last-weekday>	Rule of the form: The last [Weekday] of [Month] at [Time].

<following-date>	Rule of the form: The first [Weekday] on or after the [Day]th of [Month] at [Time].
<preceding-date>	Rule of the form: The first [Weekday] on or before the [Day]th of [Month] at [Time].

ntp server

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`ntp server <index><host>`

Adds a network time server.

Parameters

<index>	Index of the time server in the list. Up to 20 time servers are supported. Time servers are checked in the order that they appear in the list.
<host>	DNS name or IP address of the time server.

ntp server failure trap

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`ntp server failure trap`

Send a trap each time a time server synchronization failed.

`no ntp server failure trap`

Do not send a trap each time a time server synchronization failed.

config-update automatic

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`config-update automatic`

Enables scheduled configuration restore or backup.

`no config-update automatic`

Disables scheduled configuration restore or backup.

The service controller can automatically download the configuration file from a local or remote URL (restore). It is also possible to upload the current configuration to a given URL (backup). Theses operations can be done at preset times.

config-update operation

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`config-update operation (restore | backup)`

Sets the type of operation that will take place at the preset time.

config-update time

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`config-update time <time>`

Sets the time of day when the scheduled configuration operation (backup or restore) will take place.

Parameters

<time>	Time as hh:mm:ss. For example: 15:44:00.

config-update uri

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
config-update uri <uri>
```

Sets the URI where the service controller will download or upload the configuration file.

```
no config-update uri
```

Clears the configuration file URI.

config-update weekday

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
config-update weekday (everyday | monday | tuesday | wednesday | thursday |
friday | saturday | sunday)
```

Sets the day when the scheduled configuration operation (backup or restore) will take place.

snmp-server trap config-change

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
snmp-server trap config-change
```

Send a trap whenever the configuration is changed.

```
no snmp-server trap config-change
```

Do not send this trap.

snmp-server trap config-update

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
snmp-server trap config-update
```

Send a trap whenever the firmware is updated.

```
no snmp-server trap config-update
```

Do not send this trap.

logging destination

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
logging destination <name>
```

Creates a new remote destination for syslog.

```
no logging destination <name>
```

Deletes the specified syslog destination.

Parameters

<name>	Name of syslog destination. Use the name "local" to edit your local log file settings. Any other name will edit/create a remote log destination.

snmp-server trap syslog-severity

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`snmp-server trap syslog-severity`

Set the severity level of syslog messages that will trigger a trap.

`no snmp-server trap syslog-severity`

Do not send this trap.

snmp-server

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`snmp-server`

Enables the SNMP agent.

`no snmp-server`

Disables the SNMP agent.

snmp-server access port-1

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`snmp-server access port-1`

Enables SNMP access on the downstream port.

`no snmp-server access port-1`

Blocks SNMP access on the downstream port.

snmp-server allow

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`snmp-server allow <ip address>/<mask>`

Adds a host to the list of IP address from which access to the SNMP interface is permitted.

`no snmp-server allow <ip address>/<mask>`

Removes a host from the list of IP address from which access to the SNMP interface is permitted.

Parameters

<address>	IP address.
</mask>	Subnet mask in CIDR format. Specifies the number of bits in the mask.

snmp-server chassis-id

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`snmp-server chassis-id <name>`

Specifies a name to identify the service controller. By default, this is set to the serial number of the service controller.

`no snmp-server chassis-id`

Deletes the system name.

snmp-server contact

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`snmp-server contact <email>`

Specifies contact information.

`no snmp-server contact`

Deletes contact information.

Parameters

<email>	Email address.

snmp-server heartbeat period

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`snmp-server heartbeat period <seconds>`

Sets the interval between sending heartbeat traps.

Parameters

<seconds>	Heartbeat interval in seconds.

snmp-server location

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`snmp-server location <name>`

Specifies the location where the service controller is installed.

`no snmp-server location`

Deletes location information.

Parameters

<name>	Location where the service controller is installed.

snmp-server port

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`snmp-server port <port number>`

Sets the port the service controller will use to respond to SNMP requests.

Parameters

<port number>	SNMP port number. Range 1 - 65535.

snmp-server readonly

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`snmp-server readonly <community>`

Sets the read-only community string.

`no snmp-server readonly`

Deletes the read-only community string.

snmp-server readwrite

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`snmp-server readwrite <community>`

Sets the read-write community string.

`no snmp-server readwrite`

Deletes the read-write community string.

snmp-server trap

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`snmp-server trap`

Enables support for SNMP traps.

`no snmp-server trap`

Disables support for SNMP traps.

snmp-server trap community

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`snmp-server trap community <str>`

Sets the password required by the remote host that will receive the trap.

`no snmp-server trap community`

Deletes the password required by the remote host that will receive the trap.

snmp-server trap destination

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`snmp-server trap destination <host> <[port number]>`

Add a new trap destination.

`no snmp-server trap destination <host> [<port>]`

Deletes the specified trap destination.

Parameters

<host>	Sets the IP address or domain name of the host that the service controller will send traps to.
<[port number]>	SNMP port number. Range 1 - 65535. By default port 162 is used

snmp-server trap heartbeat

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`snmp-server trap heartbeat`

Enables sending of heartbeat traps at regular intervals.

`no snmp-server trap heartbeat`

Disables sending of heartbeat traps at regular intervals.

snmp-server trap link-state

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
snmp-server trap link-state
```

Send a trap when the link state changes on any interface.

```
no snmp-server trap link-state
```

Do not send this trap.

snmp-server trap snmp-authentication

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
snmp-server trap snmp-authentication
```

Send a trap each time an SNMP request fails to supply the correct community name.

snmp-server version 1

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
snmp-server version 1
```

Enable version 1

```
no snmp-server version 1
```

Disable version 1

snmp-server version 2c

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
snmp-server version 2c
```

Enable version 2c

```
no snmp-server version 2c
```

Disable version 2c

snmp-server version 3

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
snmp-server version 3
```

Enable version 3

```
no snmp-server version 3
```

Disable version 3

snmp-server access interface vlan

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
snmp-server access interface vlan <name>
```

Enables access to SNMP via the specified VLAN.

```
no snmp-server access interface vlan <name>
```

Disables access to SNMP via the specified VLAN.

Parameters

<name>	Specifies the name of the VLAN.

snmp-server access interface gre

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`snmp-server access interface gre <name>`

Enables access to SNMP via the specified GRE tunnel.

`no snmp-server access interface gre <name>`

Removes access to SNMP via the specified GRE tunnel.

snmp-server access port-2

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`snmp-server access port-2`

Enables SNMP access on the upstream port.

`no snmp-server access port-2`

Blocks SNMP access on the upstream port.

snmp-server access lan

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`snmp-server access lan`

Enables access to the management tool via the LAN port.

`no snmp-server access lan`

Blocks access to the management tool via the LAN port.

snmp-server access vpn

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`snmp-server access vpn`

Enables access to the management tool via a VPN connection.

`no snmp-server access vpn`

Blocks access to the management tool via a VPN connection.

snmp-server trap new-satellite-detected

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`snmp-server trap new-satellite-detected`

Send a trap when a new satellite is detected.

`no snmp-server trap new-satellite-detected`

Do not send a trap when a new satellite is detected.

snmp-server trap satellite-unreachable

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`snmp-server trap satellite-unreachable`

Send a trap when a satellite cannot be reached.

`no snmp-server trap satellite-unreachable`

Ignore unreachable satellites.

snmp-server user

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`snmp-server user <name>`

Creates a new SNMP user or switches to the SNMP user context with the specified user name.

`no snmp-server user <name>`

Deletes the specified SNMP user.

snmp-server notification receiver

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`snmp-server notification receiver <host>`

Creates a new SNMP notification receiver or switches to the SNMP notification receiver context with the specified IP address.

`no snmp-server notification receiver <host>`

Deletes the specified SNMP notification receiver.

soap-server

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`soap-server`

Enables the SOAP server.

`no soap-server`

Disables the SOAP server.

soap-server access interface vlan

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`soap-server access interface vlan <name>`

Enables access to SOAP via this VLAN.

`no soap-server access interface vlan <name>`

Disables access to SOAP via this VLAN.

soap-server access port-1

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
soap-server access port-1
```

Enables SOAP access on the downstream port.

```
no soap-server access port-1
```

Blocks SOAP access on the downstream port.

soap-server access port-2

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
soap-server access port-2
```

Enables SOAP access on the upstream port.

```
no soap-server access port-2
```

Blocks SOAP access on the upstream port.

soap-server allow

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
soap-server allow <ip address>/<mask>
```

Adds a host to the list of IP address from which access to the SOAP interface is permitted.

```
no soap-server allow <ip address>/<mask>
```

Removes a host from the list of IP address from which access to the SOAP interface is permitted.

Parameters

<address>	IP address.
</mask>	Subnet mask in CIDR format. Specifies the number of bits in the mask.

soap-server http authentication

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
soap-server http authentication
```

Enable the SOAP server HTTP authentication.

```
no soap-server http authentication
```

Disable the SOAP server HTTP authentication.

soap-server http authentication password

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
soap-server http authentication password
```

Set the SOAP server HTTP authentication password.

soap-server http authentication username

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`soap-server http authentication username`

Set the SOAP server HTTP authentication username.

soap-server port

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`soap-server port <port number>`

Sets the port the service controller will use to respond to SOAP requests.

Parameters

<port number> SOAP port number. Range 1 - 65535.

soap-server ssl

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`soap-server ssl`

SSL enabled for SOAP server.

`no soap-server ssl`

SSL disabled for SOAP server.

soap-server ssl with client certificate

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`soap-server ssl with client certificate`

Enable the use of client certificate with SSL for SOAP server.

`no soap-server ssl with client certificate`

Disable the use of client certificate with SSL for SOAP server.

soap-server access interface gre

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`soap-server access interface gre <name>`

Enables access to SOAP via the specified GRE tunnel.

`no soap-server access interface gre <name>`

Removes access to SOAP via the specified GRE tunnel.

soap-server access lan

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`soap-server access lan`

Enables access to the management tool via the LAN port.

`no soap-server access lan`

Blocks access to the management tool via the LAN port.

soap-server access vpn

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
soap-server access vpn
```

Enables access to the management tool via a VPN connection.

```
no soap-server access vpn
```

Blocks access to the management tool via a VPN connection.

snmp-server trap vpn-connection

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
snmp-server trap vpn-connection
```

Send a trap when a user establishes a VPN connection with the service controller.

```
no snmp-server trap vpn-connection
```

Do not send this trap.

snmp-server trap syslog-matches

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
snmp-server trap syslog-matches
```

Send a trap when syslog messages matches a specified regular expression.

```
no snmp-server trap syslog-matches
```

Do not send this trap.

snmp-server trap syslog-matches regex

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
snmp-server trap syslog-matches regex <regex>
```

Sets the regular expression used to match the syslog messages.

snmp-server trap syslog-severity level

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
snmp-server trap syslog-severity level (debug | info | notice | warning | error
| critical | alert | emergency)
```

Set the severity level of syslog messages that will trigger a trap.

snmp-server trap network-trace

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
snmp-server trap network-trace
```

Send a trap when a network trace is started or stopped.

```
no snmp-server trap network-trace
```

Do not send this trap.

firmware-update automatic

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`firmware-update automatic`

Enables scheduled firmware upgrades.

`no firmware-update automatic`

Disables scheduled firmware upgrade.

The service controller can automatically retrieve and install firmware from a local or remote URL at preset times. By placing service controller firmware on a web or ftp server, you can automate the update process for multiple units.

When the update process is triggered the service controller retrieves the first 2K of the firmware file to determine if it is different from the active version. If different, the entire firmware file is then downloaded and installed.

(Different means older or newer. This enables you to return to a previous firmware version if required).

Configuration settings are preserved during the update unless stated otherwise in the release notes for the firmware. However, all active connections will be terminated. Users will have to log in again after the service controller restarts

firmware-update start

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`firmware-update start`

Upload the firmware based on a specified URI. This URI can be set with the command: firmware-update uri.

firmware-update time

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`firmware-update time <time>`

Sets the time of day the scheduled firmware upgrade will take place.

Parameters

<time>	Time as hh:mm:ss. For example: 15:44:00.

firmware-update uri

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`firmware-update uri <uri>`

Sets the URI where the service controller will retrieve new firmware.

`no firmware-update uri`

Clears the firmware URI.

firmware-update weekday

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
firmware-update weekday (everyday | monday | tuesday | wednesday | thursday |
friday | saturday | sunday)
```

Sets the day when the scheduled firmware upgrade will take place.

snmp-server trap firmware-update

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
snmp-server trap firmware-update
```

Send a trap on firmware update.

```
no snmp-server trap firmware-update
```

Do not send a trap on firmware update.

ip name-server

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

ip name-server *<primary>* [*<secondary>*] [*<third>*]

Sets the primary and secondary DNS servers overriding dynamically assigned ones.

Parameters

<primary>	IP address of the primary DNS server.
<secondary>	IP address of the secondary DNS server.
<third>	IP address of the third DNS server.

ip name-server cache

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
ip name-server cache
```

Enables the DNS cache.

```
no ip name-server cache
```

Disables the DNS cache.

Once a host name has been successfully resolved to an IP address by a remote DNS server, it is stored in the cache. This speeds up network performance, as the remote DNS server now does not have to be queried for subsequent requests for this host.

The entry stays in the cache until:

- an error occurs when connecting to the remote host
- the time to live (TTL) of the DNS request expires
- the service controller is restarted.

ip name-server dynamic

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
ip name-server dynamic
```

Enables dynamic assignment of DNS servers.

```
no ip name-server dynamic
```

Disables dynamic DNS assignment.

ip name-server interception

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
ip name-server interception
```

Intercepts all DNS requests from users and relays them to configured servers.

```
no ip name-server interception
```

Process DNS requests addressed to this device only.

ip name-server switch-on-servfail

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
ip name-server switch-on-servfail
```

Switch to next server when server failure is received.

```
no ip name-server switch-on-servfail
```

Do not switch to next server when server failure is received.

ip name-server switch-over

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
ip name-server switch-over
```

Switch over to primary when active.

```
no ip name-server switch-over
```

Do not switch over to primary when active.

ip name-server logout-info

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
ip name-server logout-info <host> <ip address>
```

Sets the logout host name and the logout IP address.

access controller shared secret

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
access controller shared secret <secret>
```

Sets the shared secret used to communicate with the service controller.

```
no access controller shared secret
```

Sets the shared secret used to communicate with the access controller.

The service controller will only accept authentication/location-aware information from satellites that have a matching shared secret to its own.

radius-server profile

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`radius-server profile <name>`

Creates a new RADIUS profile or switches to the RADIUS context with the specified profile name.

`no radius-server profile <name>`

Deletes the specified RADIUS profile.

access controller

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`access controller`

Switches to the access controller context.

certificate ipsec ca

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`certificate ipsec ca <uri>`

Loads a new CA certificate from the specified URI.

The URI can be local:

- local://FILENAME

or remote

- ftp://host/path

certificate ipsec local

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`certificate ipsec local <uri> <password>`

Loads a new local certificate from the specified URI.

`no certificate ipsec local`

Removes the local certificate.

The URI can be local:

- local://FILENAME

or remote

- ftp://host/path

certificate ipsec revocation

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`certificate ipsec revocation <uri>`

Loads a new CRL file from the specified URI.

The URI can be local:

- local://FILENAME

or remote

- ftp://host/path

certificate ssl

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`certificate ssl <uri> <password>`

Loads a new SSL certificate using the URI.

session profile default

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`session profile default`

Switches to the session profile context.

session profile

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`session profile <name>`

Switches to the session profile context.

`no session profile <name>`

Remove a session profile.

show session profile

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`show session profile`

Display all session profiles.

remote configuration

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`remote configuration (radius)`

Switches to the RADIUS remote configuration context.

discovery protocol

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`discovery protocol`

Enables broadcast of device information for interoperability with CDP-enabled networking hardware.

`no discovery protocol`

Disable broadcast of device information.

discovery protocol device-id

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`discovery protocol device-id <name>`

Overwrite the device-id field of information packets (the service controller serial number is not used).

`no discovery protocol device-id`

Do not overwrite the device-id field of information packets (use the service controller serial number).

service controller ap authentication credentials

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`service controller ap authentication credentials <username> <password>`

When the RADIUS authentication source is selected, this option specifies the RADIUS username and password assigned to the service controller.

`no service controller ap authentication credentials`

Clears the RADIUS username/password.

service controller ap authentication enable

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`service controller ap authentication enable`

Enables authentication of discovered controlled APs.

`no service controller ap authentication enable`

Disables AP authentication.

service controller ap authentication file

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`service controller ap authentication file <name>`

Sets the file to use for authentication of controlled access points. This must be an ASCII file with one or more MAC addresses in it. Each address must appear on a separate line.

service controller ap authentication radius-server

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`service controller ap authentication radius-server <name>`

Sets the RADIUS profile to use for authentication of controlled access points.

service controller ap authentication refresh-rate

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`service controller ap authentication refresh-rate <number>`

Specifies the interval at which the service controller retrieves authentication list entries from the selected authentication source(s).

service controller ap authentication source file

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
service controller ap authentication source file
```

Enables the use of a file authentication source.

```
no service controller ap authentication source file
```

Disables the use of a file authentication source.

service controller ap authentication source local

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
service controller ap authentication source local
```

Enables the use of local authentication source.

```
no service controller ap authentication source local
```

Disables the use of local authentication source.

service controller ap authentication source radius

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
service controller ap authentication source radius
```

Enables the use of RADIUS authentication source.

```
no service controller ap authentication source radius
```

Disables the use of RADIUS authentication source.

service controller discovery

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
service controller discovery
```

Enable service controller discovery.

```
no service controller discovery
```

Disable service controller discovery.

service controller discovery interface internet-port

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
service controller discovery interface internet-port
```

Allow discovery on the LAN interface.

```
no service controller discovery interface internet-port
```

Allow discovery on the LAN interface.

service controller discovery interface lan-port

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
service controller discovery interface lan-port
```

Allow discovery on the LAN interface.

```
no service controller discovery interface lan-port
```

Allow discovery on the LAN interface.

service controller primary

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
service controller primary
```

Become the Primary service controller.

```
no service controller primary
```

Become a secondary service controller.

service controller primary ip addr

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
service controller primary ip addr <ip address>
```

Configure a static ip address for the primary service controller.

service controller priority

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
service controller priority <number>
```

Sets the discovery priority of this device.

service controller provisioning

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
service controller provisioning
```

Enable the AP provisioning system.

```
no service controller provisioning
```

Disable the AP provisioning system.

bandwidth control internet-port

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
bandwidth control internet-port
```

Enables bandwidth control on the Internet port.

```
no bandwidth control internet-port
```

Disables bandwidth control on the Internet port.

bandwidth control internet-port high

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
bandwidth control internet-port high <min-tx-%> <min-rx-%> <max-tx-%> <max-rx-%>
```

Sets the bandwidth rates (Tx minimum, Tx maximum, Rx minimum, and Rx maximum) for traffic classed as High.

bandwidth control internet-port low

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`bandwidth control internet-port low <min-tx-%> <min-rx-%> <max-tx-%> <max-rx-%>`

Sets the bandwidth rates (Tx minimum, Tx maximum, Rx minimum, and Rx maximum) for traffic classed as Low.

bandwidth control internet-port max-rate

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`bandwidth control internet-port max-rate<transmit>)<receive>)`

Sets the maximum transmit and receive rates on the Internet port in kbps.

These settings enable you to limit the total incoming or outgoing data rate on the Internet port. If traffic exceeds the rate you set for short bursts, it is buffered. Long overages will result in data being dropped. To utilize the full available bandwidth, the transmit and receive limits should be set to match the incoming and outgoing data rates on the Internet port.

Parameters

<transmit>	Sets the maximum transmit rate in kbps.
<receive>	Sets the maximum receive rate in kbps.

About bandwidth control

Bandwidth rates for each level are defined by taking a percentage of the maximum transmit and receive rates defined for the Internet port. Each bandwidth level has four rate settings:

- Transmit rate - guaranteed minimum: This is the minimum amount of bandwidth that will be assigned to a level as soon as outgoing traffic is present on the level.
- Transmit rate - maximum: This is the maximum amount of outgoing bandwidth that can be consumed by the level. Traffic in excess will be buffered for short bursts, and dropped for sustained overages.
- Receive rate - guaranteed minimum: This is the minimum amount of bandwidth that will be assigned to a level as soon as incoming traffic is present on the level.
- Receive rate - maximum: This is the maximum amount of incoming bandwidth that can be consumed by the level. Traffic in excess will be buffered for short bursts, and dropped for sustained overages.

Bandwidth levels are arranged in order of priority from Very High to Low. Priority determines how bytesToWrite bandwidth is allocated once the minimum rate has been met for each level. Free bandwidth is always assigned to the higher priority levels first.

Assigning traffic to bandwidth levels

- User traffic is assigned to a bandwidth level on a per-VAP (VSC) basis.
- Management traffic (RADIUS, SNMP, management tool admin sessions) is assigned to bandwidth level Very High and cannot be changed.
- All traffic assigned to a particular bandwidth level shares the allocated bandwidth for that level.

bandwidth control internet-port normal

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`bandwidth control internet-port normal <min-tx-%> <min-rx-%> <max-tx-%> <max-rx-%>`

Sets the bandwidth rates (Tx minimum, Tx maximum, Rx minimum, and Rx maximum) for traffic classed as Normal.

bandwidth control internet-port very-high

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`bandwidth control internet-port very-high <min-tx-%> <min-rx-%> <max-tx-%> <max-rx-%>`

Sets the bandwidth rates (Tx minimum, Tx maximum, Rx minimum, and Rx maximum) for traffic classed as Very High.

ip route gateway

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`ip route gateway<destination>/<mask> <gateway> <[metric]>`

Adds a static route.

`no ip route gateway <destination>/<mask> <gateway> <[metric]>`

Removes the specified static route.

Parameters

<destination>	Traffic addressed to this IP address will be routed.
<mask>	Indicates the number of bits in the destination address that is checked for a match.
<gateway>	Indicates the IP address of the gateway the service controller will forward routed traffic to. The gateway address must be on the same subnet as one of the available interfaces (Internet port or LAN port).
<metrix>	Indicates the priority of a route. If two routes exist for a destination address then the service controller chooses the one with the lower metric.

firewall mode

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`firewall mode (high|low|none)`

Sets the firewall mode.

Parameters

`high`	Permits all outgoing traffic. Blocks all externally initiated connections.
`low`	Permits all incoming and outgoing traffic, except for NetBIOS traffic. Use this option if you require active FTP sessions.
`none`	Disables the firewall.

show user profiles

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`show user profiles [<pattern>]`

Display current local users.

show user profiles details

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`show user profiles details <name>`

Display detailed information about one user.

user profile

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`user profile <name>`

Adds or edits the specified username in the local user list.

`no user profile <name>`

Removes the specified username from the local user list.

renew user profile subscription

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`renew user profile subscription [<username>]`

Renew a user with its subscription plan.

dot1x reauth

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`dot1x reauth`

Enable this option to force 802.1X client stations to reauthenticate.

`no dot1x reauth`

Disables 802.1X reauthentication.

dot1x reauth period

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`dot1x reauth period (15m | 30m | 1h | 2h | 4h | 8h | 12h)`

Sets the 802.1X reauthentication interval. Client stations must reauthenticate when this interval expires.

dot1x reauth terminate

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`dot1x reauth terminate`

Enable this option to allow client stations to remain connected during re-authentication. Client traffic is blocked only when re-authentication fails.

```
no dot1x reauth terminate
```

Disabled this option to block client traffic during re-authentication and only activate traffic again if authentication succeeds.

dot1x supplicant timeout

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
802.1x supplicant time-out <seconds>
```

Sets the 802.1X supplicant time-out.

Parameters

<seconds>	time-out in seconds.

dynamic key

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
dynamic key
```

Enables dynamic key support for 802.1X and WPA.

```
no dynamic key
```

Disables dynamic key support for 802.1X and WPA.

dynamic key interval

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
dynamic key interval (5m | 10m | 15m | 30m | 1h | 2h | 4h | 8h | 12h)
```

Specifies how often (in minutes or hours) that the group (broadcast) key is changed for 802.1X and WPA.

key chain

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
key chain <name>
```

Switch to the specified key chain or create a new key chain.

```
no key chain <name>
```

Remove the specified key chain.

config-version

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
config-version <string>
```

Sets a string to identify the user configuration version.

radius-server accounting session

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
radius-server accounting session <number>
```

Set the maximum number of accounting sessions.

radius-server client

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
radius-server client
```

Enable radius clients list.

```
no radius-server client
```

Disable radius clients list.

radius-server local eap-peap

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
radius-server local eap-peap
```

Allow EAP-PEAP.

```
no radius-server local eap-peap
```

Disallow EAP-PEAP.

radius-server local eap-tls

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
radius-server local eap-tls
```

Allow EAP-TLS.

```
no radius-server local eap-tls
```

Disallow EAP-TLS.

radius-server local eap-ttls

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
radius-server local eap-ttls
```

Allow EAP-TTLS.

```
no radius-server local eap-ttls
```

Disallow EAP-TTLS.

radius-server local pap

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
radius-server local pap
```

Allow PAP.

```
no radius-server local pap
```

Disallow PAP.

radius-server ssid detection nas-id

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
radius-server ssid detection nas-id
```

Use NAS-ID for SSID detection.

```
no radius-server ssid detection nas-id
```

Do not use NAS-ID for SSID detection.

show radius-server

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
show radius-server
```

Display current RADIUS server configuration.

active-directory check attribute

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
active-directory check attribute <ldapattr>
```

Set the name of the AD attribute to check for.

```
no active-directory check attribute
```

Clear the name of the AD attribute to check for.

active-directory check user access

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
active-directory check user access
```

Check AD for user access.

```
no active-directory check user access
```

Do not check AD for user access.

active-directory device name

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
active-directory device name <name>
```

Set the device NetBIOS name.

```
no active-directory device name
```

Clear the device NetBIOS name.

active-directory domain

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
active-directory domain <domain>
```

Set the AD Windows domain.

```
no active-directory domain
```

Reset the AD Windows domain.

active-directory group

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`active-directory group <name>`

Create or go to an Active Directory group.

`no active-directory group <name>`

Remove an Active Directory group.

active-directory group order

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`active-directory group order <number> <name>`

Reorder an Active Directory group.

active-directory join

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`active-directory join <username> <password>`

Join with Active Directory.

show active-directory

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`show active-directory`

Display Active Directory settings.

show active-directory group

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`show active-directory group <name>`

Display details about an Active Directory group.

radius-server client

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`radius-server client <ip address>/<mask> <secret>`

Add a new radius client.

`no radius-server client <ip address>/<mask>`

Delete an existing radius client.

user tracking

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`user tracking`

Enable capture of usage data.

`no user tracking`

Disable capture of usage data.

user tracking destination

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`user tracking destination <host>`

Specify to where the detailed syslog packets should be sent.

user tracking filter

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`user tracking filter <filter>`

A comma-separated list of filters (username or subnet).

user tracking port

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`user tracking port <number>`

Specify to which UDP port capture data should be sent.

persistent user information

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`persistent user information`

Save user account information locally .

`no persistent user information`

Do not save user account information locally.

persistent user information period

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`persistent user information period <number>`

Period, in minutes, at which to update user information.

client data tunnel security

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`client data tunnel security (hmac | key)`

Specify the security strength of the client data tunnel.

managed map max

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`managed map max <num>`

Set the maximum number of APs to manage.

igmp proxy

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`igmp proxy`

Enable IGMP proxy.

`no igmp proxy`

Disable IGMP proxy.

igmp proxy downstream interface

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`igmp proxy downstream interface <interface>`

Set the downstream IGMP port.

igmp proxy upstream interface

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`igmp proxy upstream interface <interface>`

Set the upstream IGMP port.

rf-id aeroscout

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`rf-id aeroscout`

Enable AeroScout tag processing.

`no rf-id aeroscout`

Disable AeroScout tag processing.

Access Controller context

Path: View > Enable > Config > Access Controller

All global access controller configuration takes place here.

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
end
```

Switches to parent context.

ads presentation

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
ads presentation
```

Enable advertisement display at regular intervals for authenticated users.

```
no ads presentation
```

Disable advertisement display for authenticated users.

ads presentation interval

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
ads presentation interval <number>
```

Control the advertisement display interval.

station allocate source ip address

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
station allocate source ip address
```

Allow dynamic IP addresses.

```
no station allocate source ip address
```

Disallow dynamic IP addresses.

Enable this option to provide network address translation for client stations with static IP addresses. This permits the service controller to assign an alias address to the client that puts it on the same subnet as the VSC the client is associated with. This option cannot be used if NAT is enabled on the Internet port.

station allow any ip address

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
station allow any ip address
```

Enable this option to permit wireless client stations that are using a static IP address to connect to the service controller, even if they are on a different subnet.

```
no station allow any ip address
```

Do not allow client stations with any IP addresses to connect.

This option enables users to access the wireless network without reconfiguring their networking settings. For example, by default the service controller creates the wireless network on the subnet 192.168.1.0. If a client station is pre-configured with the address 10.10.4.99, it will still be able to connect to the service controller without changing its address, or its settings for DNS server and default gateway.

station free access

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
station free access
```

When enabled, all users are automatically granted access when the RADIUS server is down or unreachable.

```
no station free access
```

Users cannot connect when the RADIUS server is unreachable.

Once the RADIUS server is available again, free user sessions remain active until the user logs out. This does not apply to users using 802.1x or WPA.

station http proxy support

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
station http proxy support
```

Enables support for client stations that are configured to use a proxy server for HTTP and HTTPS, without requiring users to reconfigure their systems.

```
no station http proxy support
```

Disables support for client stations that are configured to use a proxy server for HTTP and HTTPS.

station idle detection

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
station Idle detection <interval> <count>
```

The service controller continuously polls authenticated client stations to ensure they are active. If no response is received and the number of retries is reached, the client station is disconnected.

Parameters

<interval>	Specify how long to wait between polls.
<retries>	Specify how many polls a client station can fail to reply to before it is disconnected.

Description

This feature enables the service controller to detect if two client stations are using the same IP address but have different MAC addresses. If this occurs, access is terminated for this IP address removing both stations from the network.

Changing these values may have security implications. A large interval provides a greater opportunity for a session to be hijacked.

The initial query is always done after the client station has been idle for 60 seconds. If there is no answer to this query, the settings for Interval and Retries are used to control additional retries.

system accounting

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`system accounting`

Enables RADIUS accounting support.

`no system accounting`

Disables RADIUS accounting support.

remember delay

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`remember delay <number>`

Length of time to remember users. Users who return later than this delay interval, are presented with the login page instead of being re-authenticated.

remember html users

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`remember html users`

Enables support for remembering (automatically re-authenticating) html-authenticated users who leave the network but return within the remember delay interval.

`no remember html users`

Disables support for remembering html-authenticated users.

worldpay installation id

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`worldpay installation id <string>`

Set the installation ID for the WorldPay payment service.

worldpay payment response password

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`worldpay payment response password <string>`

Set the payment response password for the WorldPay payment service.

worldpay payment url

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`worldpay payment url <string>`

Set the payment URL for the WorldPay payment service.

authorize_net installation id

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`authorize_net installation id <string>`

Set the login ID for the Authorize.Net payment service.

authorize_net payment url

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`authorize_net payment url <string>`

Set the payment URL for the Authorize.Net payment service.

authorize_net transaction key

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`authorize_net transaction key <string>`

Set the transaction key for the Authorize.Net payment service.

ads presentation with frameset

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`ads presentation with frameset`

Enables the ads presentation to redirect to frameset-ads-page instead of ads-page.

`no ads presentation with frameset`

Disables the frameset for ads presentation, causing ads presentation to only use ads-page.

authentication http

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`authentication http <number>`

Specifies the port number the service controller will use to provide standard HTTP access to the management tool.

HTTP connections made to this port are met with a warning and the browser is redirected to the secure web server port. By default this parameter is set to port 80.

authentication https

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`authentication https <number>`

Specifies the port number the service controller will use to provide secure access to the management tool (HTTPS). By default this parameter is set to port 443.

noc access internet

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`noc access internet`

Accept authentication requests on the Internet port.

`no noc access internet`

Do not accept authentication requests on the Internet port..

noc access vpn

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`noc access vpn`

Accept authentication requests on VPN connections.

`no noc access vpn`

Do not accept authentication requests on VPN connections.

noc allow

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`noc allow <ip address>/<mask>`

Adds an IP address or subnet to the list of destinations that the service controller will accept user login authentication requests from when NOC authentication is active.

`no noc allow <ip address>/<mask>`

Removes the specified IP address or subnet from the list of destinations that the service controller will accept user login authentication requests from when NOC authentication is active.

When the list is empty, authentication requests are accepted from any address.

noc authentication

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`noc authentication`

Enables support for NOC authentication.

`no noc authentication`

Disables support for NOC authentication.

secure login

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`secure login`

Enables secure login.

`no secure login`

Disables secure login.

sslv2 authentication

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`sslv2 authentication`

Enables SSLv2 authentication.

`no sslv2 authentication`

Disables SSLv2 authentication.

noc access interface vlan

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`noc access interface vlan <name>`

Adds the specified VLAN to the list of interfaces that authentication requests are accepted on.

`no noc access interface vlan <name>`

Removes the specified VLAN from the list of interfaces that authentication requests are accepted on.

noc access interface gre

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`noc access interface gre <name>`

Adds the specified GRE tunnel to the list of interfaces that authentication requests are accepted on.

`no noc access interface gre <name>`

Removes the specified GRE tunnel from the list of interfaces that authentication requests are accepted on.

ipass id

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`ipass id <name>`

Specifies the WISPr location ID assigned to the service controller.

`no ipass id`

Deletes the WISPr location ID assigned to the service controller.

ipass name

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`ipass name <name>`

Specifies the WISPr location name assigned to the service controller.

`no ipass name`

Deletes the WISPr location name assigned to the service controller.

wispr abort login url

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`wispr abort login url <url>`

Specifies the WISPr abort login url assigned to the service controller.

`no wispr abort login url`

Deletes the WISPr abort login url assigned to the service controller.

wispr login url

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`wispr login url <url>`

Specifies the WISPr login url assigned to the service controller.

`no wispr login url`

Deletes the WISPr login url assigned to the service controller.

wispr logoff url

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`wispr logoff url <url>`

Specifies the WISPr logoff url assigned to the service controller.

`no wispr logoff url`

Deletes the WISPr logoff url assigned to the service controller.

access-list

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`access-list <index> <rule>`

Adds a new rule to an access list at the specified index position.

`no use access-list`

Do not use an access list.

Parameters

`index`	Index position of the rule within the access list.
`rule`	Access list rule definition in the format: <*listname*>[,OPTIONAL],<*action*>,<*protocol*>,<*address*>,<*port*>[,<*account*>[,<*interval*>]]
<listname>	Specifies a name (up to 32 characters long) to identify the access list this rule applies to. If a list with this name does not exist, a new list is created. If a list with this name exists, the rule is added to it.
`OPTIONAL`	Allows the access list to be activated even if this rule fails to initialize. For example, if you specify a rule that contains an address which cannot be resolved for some reason, the other rules that make up the access list will still be initialized. If you do not specify optional, a failed rule will cause the entire list to fail. Critical access list definitions (such as for a remote login page, certificates) should not use the OPTIONAL setting because if these definitions fail to initialize there will be no indication in the log.
<action>	Specifies what action the rule takes when it matches incoming traffic. Two options are available:

- ACCEPT - Allow traffic matching this rule.
- DENY - Reject traffic matching this rule.
- WARN - Redirect traffic matching this rule to an error page.

<protocol>	Specify the protocol to check: tcp, udp, icmp, all
<address>	Specify one of the following:

- IP address or domain name (up to 107 characters in length)
- Subnet address. Include the network mask as follows: address/subnet mask For example: 192.168.30.0/24
- Use the keyword **all** to match any address.
- Use the keyword **none** if the protocol does not take an address range (ICMP for example).

<port> Specify a specific port to check or a port range as follows:

- none: Used with ICMP (since it has no ports).
- all: Check all ports.
- 1-65535[:1-65535] - Specify a specific port or port range.

<account> Specify the name of the user account the service controller will send billing information to for this rule. Account names must be unique and can be up to 32 characters in length.

<interval> Specify time between interim accounting updates. If you do not enable this option, accounting information is only sent when a user connection is terminated. Range: 5-99999 seconds in 15 second increments.

use access-list

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`use access-list <listname>`

Specifies the name of the access list to use.

`no use access-list`

Do not use an access list.

use access-list unauth

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`use access-list unauth <listname>`

Specifies the name of the access list to use for unauthenticated stations (list disappears once authenticated).

`no use access-list unauth`

Do not use an access list for unauthenticated stations (list disappears once authenticated).

config file

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`config file <url>`

Specifies the URL that points to a new configuration file to load.

`no config file`

Do not load a new configuration file.

http proxy upstream

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`http proxy upstream <string>`

Specifies the host:port of the HTTP Proxy Upstream server.

`no http proxy upstream`

Do not use an HTTP Proxy Upstream server.

https ssl certificate

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`https ssl certificate <url>`

Specifies the URL that points to an SSL certificate that will replace the default certificate on the service controller.

`no https ssl certificate`

Do not load a custom SSL certificate.

mac-address

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`mac-address <macaddr> [<username>] [<password>]`

Adds a MAC address to the local configuration list.

When the MAC authentication option is enabled (in a VAP (VSC) profile), you can define local configuration settings to validate MAC addresses.

Parameters

`macaddr`	MAC address of the device as 12 hexadecimal numbers, with the values 'a' to 'f' in lowercase. For example: 0003520a0f01.
`username`	Username assigned to the device.
`password`	Password assigned to the device.

fail page

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`fail page <url>`

Specifies the URL of a new fail page.

`no fail page`

No new fail page. Use default.

goodbye url

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`goodbye url <url>`

Specifies the URL of a goodbye page.

`no goodbye url`

No goodbye page.

ipass login url

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`ipass login url <url>`

Specifies the URL of the IPass login page. The service controller will automatically redirect users with IPass client software to this page.

`no ipass login url`

No IPass login URL.

login error url

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`login error url <url>`

Specifies the URL of a login error page.

`no login error url`

No login error page.

login page

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`login page <url>`

Specifies the URL of the new login page.

`no login page`

No new login page. Use default.

login url

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`login url <url>`

Specifies the URL of a remote login page.

`no login url`

No remote login page.

logo

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`logo <url>`

Specifies the URL of a new logo.

`no logo`

No new logo. Use default.

messages

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`messages <url>`

Specifies the URL of a new message file.

`no messages`

No new messages file. Use default.

noc ssl ca-certificate

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`noc ssl ca-certificate <url>`

Specifies the URL of the certificate from the certificate authority (CA) that issued the NOC certificate.

`no noc ssl ca-certificate`

No CA certificate.

noc ssl certificate

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`noc ssl certificate <url>`

Specifies the URL of the certificate issued to the application on the remote web server that will send user info to the service controller for authentication.

`no noc ssl certificate`

No certificate.

session page

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`session page <url>`

Specifies the URL of a new session page.

`no session page`

No new session page. Use default.

transport page

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`transport page <url>`

Specifies the URL of a new transport page.

`no transport page`

No new transport page. Use default.

welcome url

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`welcome url <url>`

Specifies the URL of a welcome page.

`no welcome url`

No welcome page.

notify user location changes

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`notify user location changes`

Notify RADIUS on location changes.

`no notify user location changes`

Do not notify RADIUS on location changes.

Default Session profile context

Path: View > Enable > Config > Default Session profile

This context provides attributes that define settings for user sessions. Most of these attributes can be overridden by adding settings to a user RADIUS account.

In this context, all commands add an attribute to the list, in some cases (access-list & mac-address) several entries are added. The "no" form will remove the attributes.

accounting interim update

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`accounting interim update <number>`

Sets the default accounting interim update interval (in seconds) for all users that do not have a specific interval set in their profile.

`no accounting interim update`

Removes this attribute.

idle timeout

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`idle timeout <number>`

Sets the default idle time out for all users that do not have a specific limit set in their profile.

`no idle timeout`

Removes this attribute.

maximum input octets

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`maximum input octets <value>`

Sets the maximum input limit in octets for all users that do not have a specific limit set in their profile.

`no maximum input octets`

Removes this attribute.

maximum input packets

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`maximum input packets <number>`

Sets the maximum input limit in packets for all users that do not have a specific limit set in their profile.

`no maximum input packets`

Removes this attribute.

maximum output octets

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`maximum output octets <value>`

Sets the maximum output limit in octets for all users that do not have a specific limit set in their profile.

`no maximum output octets`

Removes this attribute.

maximum output packets

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`maximum output packets <number>`

Sets the maximum output limit in packets for all users that do not have a specific limit set in their profile.

`no maximum output packets`

Removes this attribute.

maximum total octets

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`maximum total octets <value>`

Sets the maximum total limit in octets for all users that do not have a specific limit set in their profile.

`no maximum total octets`

Removes this attribute.

maximum total packets

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`maximum total packets <number>`

Sets the maximum total limit in packets for all users that do not have a specific limit set in their profile.

`no maximum total packets`

Removes this attribute.

nat one-to-one

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`nat one-to-one`

Enables one-to-one NAT support for all users that do not have a specific value set in their profile.

`no nat one-to-one`

Removes this attribute.

session timeout

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`session timeout <number>`

Sets the default session timeout for all users that do not have a specific limit set in their profile.

`no session timeout`

Removes this attribute.

smtp redirection setup

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`<hostname>[:<port>t][,<username>,<password>]`

Sets basic SMTP redirection info: hostname[:port][,username,password].

`no smtp redirection setup`

Clears basic SMTP redirection info.

Parameters

<hostname>	Specify the IP address or domain name of the e-mail server. Maximum length is 253 characters.
<port>	Specify the port on the e-mail server to relay to. Range: 1 to 65535. Default: 25
<username>	Specify the username required to log on to the SMTP server. Maximum 32 characters.
<password>	Specify the password required to log on to the SMTP server. Maximum 32 characters.

Description

Sets the default SMTP server address for all user sessions. This attribute is used if a specific server is not set for a particular user

public ip subnet

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`public ip subnet`

Enables the use of the public IP subnet for IP Addressing for all users that do not have a specific value set in their profile.

`no public ip subnet`

Removes this attribute.

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`end`

Switches to parent context.

smtp redirection

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
smtp redirection
```

Enables SMTP proxy support.

```
no smtp redirection
```

Disables SMTP proxy support.

Session profile context

Path: View > Enable > Config > Session profile

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
end
```

Switches to parent context.

access controlled

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
access controlled
```

Set profile as 'access controlled'.

```
no access controlled
```

Set profile as not 'access controlled'.

access list

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
access list <name>
```

Set the access list.

```
use access list
```

Use this access list.

```
no use access list
```

Do not use this access list.

accounting interim update

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
accounting interim update <number>
```

Sets the default accounting interim update interval (in seconds) for all users that do not have a specific interval set in their profile.

```
use accounting interim update
```

Use attribute.

```
no use accounting interim update
```

Removes this attribute.

arp polling interval

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
arp polling interval <number>
```

Set the ARP polling interval.

`use arp polling interval`

Use the ARP polling interval.

`no use arp polling interval`

Do not use the ARP polling interval.

arp polling max count

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`arp polling max count <number>`

Set the polling ARP count.

`use arp polling max count`

Use the polling ARP count.

`no use arp polling max count`

Do not use the polling ARP count.

bandwidth level

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`bandwidth level (very-high | high | normal | low)`

Set Bandwidth level.

`use bandwidth level`

Use Bandwidth level.

`no use bandwidth level`

Don't use Bandwidth level.

egress vlan

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`egress vlan <number>`

Set the tunnel private group id.

`use egress vlan`

Use the tunnel private group id.

`no use egress vlan`

Do not use the tunnel private group id.

idle timeout

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`idle timeout <number>`

Sets the default idle time out for all users that do not have a specific limit set in their profile.

`use idle timeout`

Use this attribute.

```
no use idle timeout
```

Removes this attribute.

intercept traffic

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
intercept traffic
```

Turn on legal traffic interception.

```
no intercept traffic
```

Turn off legal traffic interception.

```
use intercept traffic
```

Use legal traffic interception.

```
no use intercept traffic
```

Do not use legal traffic interception.

max input rate

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
max input rate <number>
```

Set the maximum input rate.

```
use max input rate
```

Use the maximum input rate.

```
no use max input rate
```

Do not use the maximum input rate.

max output rate

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
max output rate <number>
```

Set the maximum output rate.

```
use max output rate
```

Use the maximum output rate.

```
no use max output rate
```

Do not use the maximum output rate.

nat one-to-one

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
nat one-to-one
```

Enables one-to-one NAT support for all users that do not have a specific value set in their profile.

```
no nat one-to-one
```

Removes this attribute.

```
use nat one-to-one
```

Use this attribute.

```
no use nat one-to-one
```

Do not use this attribute.

session profile

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
session profile <name>
```

Change this profile's name.

smtp redirection setup

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
smtp redirection setup <hostname>[:<port>t][,<username>,<password>]
```

Sets basic SMTP redirection info: hostname[:port][,username,password].

```
no smtp redirection setup
```

Clears basic SMTP redirection info.

```
use smtp redirection setup
```

Use SMTP redirection.

```
no use smtp redirection setup
```

Do not use SMTP redirection.

Parameters

<hostname>	Specify the IP address or domain name of the e-mail server. Maximum length is 253 characters.
<port>	Specify the port on the e-mail server to relay to. Range: 1 to 65535. Default: 25
<username>	Specify the username required to log on to the SMTP server. Maximum 32 characters.
<password>	Specify the password required to log on to the SMTP server. Maximum 32 characters.

Description

Sets the default SMTP server address for all user sessions. This attribute is used if a specific server is not set for a particular user.

termination action

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
termination action (logout | reauthenticate)
```

Set the termination action.

```
use termination action
```

Use the termination action.

```
no use termination action
```

Do not use the termination action.

user defined attribute

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`user defined attribute <name>:<type>:<vendor-id>:<vendor-type>:<format>:<value>`

Add a new user defined attribute.

`no user defined attribute <description>`

Add a new user-defined attribute.

Parameters

<name>	Friendly name for this attribute.
<type>	Numerical RADIUS type, 26 is Vendor-Specific.
<vendor-id>	If RADIUS type is 26, contains the Vendor-Id. Put 0 if not.
<vendor-type>	If RADIUS type is 26, contains the Vendor-Type. Put 0 if not.
<format>	Is either 'integer', 'address', 'text', 'string' or 'time'.
<value>	Contains the actual value.

Format description and values:

- integer: value is a numerical string.
- address: value is a legal IP address, or possibly a host name.
- text: value is any string of alphanumerical characters.
- string: value is a series of hexadecimal digits.
- time: value is a time string.

For related information, see RFC 2138, Section 5.

public ip subnet

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`public ip subnet`

Set profile to use the public IP subnet for IP Addressing once authenticated.

`no public ip subnet`

Removes this attribute.

`use public ip subnet`

Use this attribute.

`no use public ip subnet`

Do not use this attribute.

User Profile context

View > Enable > Config > User Profile

Use this context to modify settings for a specific user in the local user list.

Example plan and profile configuration usig CLI commands:

```
subscription plan "silver"
  use online time limit
  online time limit 60 minutes
  restrictions
  no use initial login time allocation
  use daily restriction
  daily restriction 08:00:00 17:00:00
  no use start time
  no use end time
 end
session profile "guest"
  access controlled
  idle timeout 600
  use idle timeout
  tunnel private group id ac 55
  use tunnel private group id ac
 end
user profile "zoe"
  password gadbois
  max user sessions 1
  active
  control method subscription
  subscription plan "silver"
  use access-controlled profile
  access-controlled profile "guest"
  no restrict access-controlled virtual ap
 end
```

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
end
```

Switches to parent context.

access controlled

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
access controlled
```

Make this user access controlled.

```
no access controlled
```

Make this user not access controlled.

access-controlled profile

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
access-controlled profile <name>
```

Use this session profile for this account.

```
no access-controlled profile <name>
```

Do not use this session profile for this account.

```
use access-controlled profile
```

Use the Access Controlled profiles.

```
no use access-controlled profile
```

Use the Access Controlled profiles.

access-controlled virtual ap

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
access-controlled virtual ap <name>
```

Add to the list of allowed virtual APs.

```
no access-controlled virtual ap <name>
```

Remove from the list of allowed virtual APs.

```
use access-controlled virtual ap
```

Use only allowed Virtual AP (VSC) for this profile.

```
no use access-controlled virtual ap
```

Use any Virtual AP (VSC) for this profile.

active

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
active
```

Enable this user account.

```
no active
```

Disable this user account.

chargeable user identity

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`chargeable user identity <id>`

Set the CUI.

`use chargeable user identity`

Use the CUI.

`no use chargeable user identity`

Do not use the CUI.

control method

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`control method (subscription | endtime | none)`

How is this account controlled?

egress vlan

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`egress vlan <number>`

Set the VLAN tunnel ID.

`use egress vlan`

Use the VLAN tunnel ID.

`no use egress vlan`

Do not use the VLAN tunnel ID.

end time

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`end time <time>`

Set expiration time: "YYYY-MM-DD HH:MM:SS".

idle timeout

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`idle timeout <number>`

Sets the idle timeout for this user.

`no idle timeout`

This user never times out.

max user sessions

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`max user sessions <number>`

Sets the maximum concurrent sessions for this user.

```
no max user sessions
```

This user doesn't have a maximum concurrent sessions limit.

password

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
password <secret>
```

Change the password for this user.

regular profile

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
regular profile <name>
```

Apply a non-ac profile.

```
no regular profile <name>
```

Remove a non-ac profile.

```
use regular profile
```

Use the non-Access Controlled profiles.

```
no use regular profile
```

Do not use the non-Access Controlled profiles.

regular virtual ap

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
regular virtual ap <name>
```

Add to the list of allowed virtual APs.

```
no regular virtual ap <name>
```

Remove from the list of allowed virtual APs.

```
use regular virtual ap
```

Use only allowed Virtual AP (VSC) for this profile.

session timeout

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
session timeout <number>
```

Sets the session timeout for this user.

```
no session timeout
```

This user session never times out.

subscription plan

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
subscription plan <name>
```

Set the subscription plan to use.

```
no subscription plan
```

Delete a subscription plan.

username

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
username <name>
```

Change the name for this user.

Internet interface context

Path: View > Enable > Config > Internet interface

This context provides commands for configuring Internet.

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
end
```

Switches to parent context.

duplex

Supported on: MSM710 MSM730 MSM750 MSM760

```
duplex (auto | half | full)
```

Sets the duplex mode on Internet.

Parameters

`auto`	Lets the service controller automatically set duplex mode based on the type of equipment it is connected to.
`half`	Forces the port to operate in half duplex mode.
`full`	Forces the port to operate in full duplex mode.

speed

Supported on: MSM710 MSM730 MSM750 MSM760

```
speed (auto | 10 | 100)
```

Sets the speed of Internet.

Parameters

`auto`	Lets the service controller automatically set port speed based on the type of equipment it is connected to.
`100`	Forces the port to operate at 100 mbps.
`10`	Forces the port to operate at 10 mbps.

interface vlan

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
interface vlan <id>[-<id2>]
```

Switches to the specified VLAN interface or create a new VLAN interface with the specified ID.

```
no interface vlan <id>[-<id2>]
```

Deletes the specified VLAN.

Parameters

<id>	VLAN ID. Range: 1 - 4094.
<id2>	VLAN ID. When specified, this is the last value in a range.

ipsec vlan interface

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`ipsec vlan interface <name>`

Specifies which VLAN is used by IPsec.

`no ipsec vlan interface`

Do not use a VLAN for IPsec.

LAN interface context

Path: View > Enable > Config > LAN interface

This context provides commands for configuring LAN.

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
end
```

Switches to parent context.

duplex

Supported on: MSM710 MSM730 MSM750 MSM760

```
duplex (auto | half | full)
```

Sets the duplex mode on LAN.

Parameters

`auto`	Lets the service controller automatically set duplex mode based on the type of equipment it is connected to.
`half`	Forces the port to operate in half duplex mode.
`full`	Forces the port to operate in full duplex mode.

speed

Supported on: MSM710 MSM730 MSM750 MSM760

```
speed (auto | 10 | 100)
```

Sets the speed of LAN.

Parameters

`auto`	Lets the service controller automatically set port speed based on the type of equipment it is connected to.
`100`	Forces the port to operate at 100 mbps.
`10`	Forces the port to operate at 10 mbps.

interface vlan

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
interface vlan <id>[-<id2>]
```

Switches to the specified VLAN interface or create a new VLAN interface with the specified ID.

```
no interface vlan <id>[-<id2>]
```

Deletes the specified VLAN interface.

Parameters

<id>	VLAN ID. Range: 1 - 4094.
<id2>	VLAN ID. When specified, is the last value in a range.

ipsec vlan interface

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`ipsec vlan interface <name>`

Specifies which VLAN is used by IPsec.

`no ipsec vlan interface`

Do not use a VLAN for IPsec.

WAN IP interface context

Path: View > Enable > Config > WAN IP interface

This context provides commands for configuring various IP-networking related settings.

pppoe client user

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`pppoe client user <username> <password>`

Sets the PPPoE username and password.

`no pppoe client user`

Deletes the PPPoE username.

Parameters

<username>	The username assigned to you by your ISP. The service controller will use this username to log on to your ISP when establishing a PPPoE connection.
<password>	The password assigned to you by your ISP. The service controller will use this username to log on to your ISP when establishing a PPPoE connection.

ip address mode

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`ip address mode (dhcp | pppoe | static | none)`

Sets the IP addressing mode for Internet.

Parameters

`dhcp`	Dynamic host configuration protocol. The DHCP server will automatically assign an address to the service controller, which functions as a DHCP client.
`pppoe`	Point-to-point protocol over Ethernet. The PPPoE server will automatically assign an IP address to the service controller. You need to supply a username and password so the service controller can log on.
`static`	This option enables you to manually assign an IP address to the service controller.
`none`	No IP address.

ip address

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`ip address <ip address>/<mask>`

Sets a static IP address for the port.

Parameters

<address>	IP address.
</mask>	Subnet mask in CIDR format. Specifies the number of bits in the mask.

ip nat

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
ip nat
```

Enables Network Address Translation.

```
no ip nat
```

Disables Network Address Translation.

nat limit port range

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
nat limit port range
```

Reserves a range of TCP and UDP ports for each user starting at port 5000.

```
no nat limit port range
```

Use any port for NAT.

All outgoing traffic for the user is mapped within the range. Applications that set an incoming port (Active FTP, for example) may choose a port that is outside of the allocated port range. If you enable this feature you should not assign static NAT mappings in the range 5000 to 32768.

nat limit port range size

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
nat limit port range size <number>
```

Determine the size of the range to use per user, this will limit the number of user authentication supported if too high.

ip address dhcp client-id

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
ip address dhcp client-id <id>
```

Specifies an ID to identify the service controller to a DHCP server. This parameter is not required by all ISPs.

```
no ip address dhcp client-id
```

Deletes the specified DHCP client id.

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
end
```

Switches to parent context.

pppoe auto-reconnect

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
pppoe auto-reconnect
```

The service controller will automatically attempt to reconnect if the connection is lost.

```
no pppoe auto-reconnect
```

The service controller will not automatically attempt to reconnect if the connection is lost.

pppoe mru

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
pppoe mru <bytes>
```

Specifies the maximum receive unit.

Changes to this parameter should only be made according to the recommendations of your ISP. Incorrectly setting this parameter can reduce the throughput of your Internet connection.

Parameters

<bytes>	Maximum size (in bytes) of a PPPoE packet when receiving. Range: 500 - 1500 bytes.

pppoe mtu

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
pppoe mtu <bytes>
```

Specifies the maximum transmit unit.

Changes to this parameter should only be made according to the recommendations of your ISP. Incorrectly setting this parameter can reduce the throughput of your Internet connection.

Parameters

<bytes>	Maximum size (in bytes) of a PPPoE packet when transmitting. Range: 500 - 1500 bytes.

pppoe unnumbered

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
pppoe unnumbered
```

Enable unnumbered mode.

```
no pppoe unnumbered
```

Disable unnumbered mode.

This feature is useful when the service controller is connected to the Internet and NAT is not being used. Instead of assigning two IP addresses to the service controller, one to the Internet port and one to the LAN port, both ports can share a single IP address. This is especially useful when a limited number of IP addresses are available to you.

ip nat outside source static

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
ip nat outside source static (tcp|udp) <visible-port> <internal-addr>
<internal-port>
```

Adds a static NAT mapping which routes the specified incoming traffic to the specified IP address on the internal network.

Parameters

`tcp | udp`	Selects the protocol that the mapping will operate on.
<visible-port>	The protocol port number that the incoming traffic uses.

<internal addr>	IP address of the device on the internal network that traffic will be routed to.
<internal-port>	The protocol port number that the incoming traffic will be mapped to.

ip rip authentication key-chain

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
ip rip authentication key-chain <name>
```

Specifies a keyed MD5 chain.

```
no ip rip authentication key-chain
```

Do not use this Keyed MD5 chain.

ip rip authentication mode

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
ip rip authentication mode (md5 | text)
```

Select RIPv2 authentication mode.

```
no ip rip authentication mode
```

Use no RIPv2 authentication.

ip rip authentication string

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
ip rip authentication string <secret>
```

Sets the RIP shared password.

```
no ip rip authentication string
```

Clears the RIP shared password.

passive-interface

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
passive-interface
```

Sets RIP to operate in passive mode (listen for routing broadcasts to update the routing table, but do not broadcast own routes).

```
no passive-interface
```

Sets RIP to operate in active mode (listen for routing broadcasts to update the routing table, and also broadcast own routes).

router rip

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
router rip
```

Enable RIP.

```
no router rip
```

Disable RIP.

ip address alternate

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`ip address alternate <ip address> [<ip address>]`

Assigns an alternate IP addresses to the Internet port. The address must be valid on the Internet.

`no ip address alternate <ip address> [<ip address>]`

Deletes the specified alternate IP address.

The service controller uses these addresses to support its one-to-one NAT feature. The service controller will not respond to pings directed at these IP addresses:

LAN IP interface context

Path: View > Enable > Config > LAN IP interface

This context provides commands for configuring various IP-networking related settings for the LAN interface.

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
end
```

Switches to parent context.

ip address

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
ip address <ip address>/<mask>
```

Sets a static IP address for the port.

Parameters

<address>	IP address.
</mask>	Subnet mask in CIDR format. Specifies the number of bits in the mask.

ip address management

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
ip address management <ip address>/<mask>
```

Sets a management IP address for this device.

Parameters

<address>	IP address.
</mask>	Subnet mask in CIDR format. Specifies the number of bits in the mask.

passive-interface

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
passive-interface
```

Sets RIP to operate in passive mode (listen for routing broadcasts to update the routing table, but do not broadcast own routes).

```
no passive-interface
```

Sets RIP to operate in active mode (listen for routing broadcasts to update the routing table, and also broadcast own routes).

router rip

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
router rip
```

Enable RIP.

```
no router rip
```

Disable RIP.

RADIUS remote configuration context

Path: View > Enable > Config > RADIUS remote configuration

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`end`

Switches to parent context.

active

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`active`

Use a RADIUS server to fetch configuration information for the public access network.

`no active`

Do not use a RADIUS for remote configuration.

credentials

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`credentials <username> <password>`

Sets the username/password to use for RADIUS configuration.

`no credentials`

Resets the username/password to use for RADIUS configuration.

interval

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`interval <number>`

Sets the intervals at which the service controller will retrieve configuration information from the RADIUS server.

radius server profile

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`radius server profile <name>`

Sets the RADIUS profile to use.

`no radius server profile`

Do not use a RADIUS profile.

Virtual AP context

Path: View > Enable > Config > Virtual AP

This context provides commands for configuring Virtual AP profiles (VAP (VSC)s).

By default one profile exists with the name "". This is the default profile and cannot be deleted.

The following example shows how to add a new VAP (VSC) with egress mapped to an existing VLAN named "hongkong":

CLI(config)# virtual ap newap

CLI(virtual-ap)# access control

CLI(virtual-ap)# egress any vlan hongkong

CLI(virtual-ap)# ssid name "newap"

CLI(virtual-ap)# ingress ssid

CLI(virtual-ap)# bandwidth high

CLI(virtual-ap)# end

CLI(config)#

virtual ap name

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`virtual ap name <name>`

Change the VAP (VSC) name.

access control

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`access control`

Sets this profile to use the services of the service controller's access control mechanism for authentication and control of client sessions.

`no access control`

Do not provide access control with this VAP (VSC).

When enabled

- The service controller provides a variety of methods for user authentication, including: MAC, 802.1x, and HTML via either the local user list or a RADIUS server.
- Egress traffic can be routed based on the user state: authenticated, unauthenticated, or intercepted.

When disabled

- The service controller does not perform user authentication, either via RADIUS or the local user list. All authentication must be handled by a remote device.
- All wireless traffic is bridged to an egress VLAN.
- No access controller functions are available. This means no support for RADIUS attributes for the service controller.
- 802.1x support is available, including support for RADIUS attributes for users.

force centralize data

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
force centralize data
```

Force centralization of wireless client traffic when the AP is L2 connected to the LAN port of the service controller.

```
no force centralize data
```

Automatically determine if centralization of wireless client traffic is required.

ingress interface

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
ingress vlan <name>
```

Sets the specified interface as the ingress interface traffic will be accepted on.

This command takes a *selector* as its input. A selector is used to differentiate traffic, and decide which parameters should be used to select the VAP (VSC) this user/traffic applies to.

egress unauthenticated

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
egress ( unauthenticated | authenticated | intercepted ) ( default | vlan <vlan-name> | gre <gre-name>)
```

Sets the output interface that this profile forwards data traffic to.

Parameters

`unauthenticated`	This is any traffic from client stations that have not attempted to be authenticated by the service controller. For example, a client station that fails to authenticate via 802.1x is not considered to be unauthenticated.
`authenticated`	This is any traffic from client stations that have been authenticated by the service controller and given access to the public access interface.
`intercepted`	Traffic from specific users can be intercepted and redirected. To enable traffic interception for a specific user, you must specify the appropriate setting in the their RADIUS account. See the Management and Configuration Guide for details.
`default`	Sends traffic without specifying a specific interface. The interface that is used will be selected by the routing module based on the traffic destination
<vlan-name>	Sends traffic tagged with the VLAN ID defined for the specified VLAN name.
<gre-name>	Sends traffic on the specified GRE tunnel.

guest-mode

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
guest-mode
```

Enables broadcast of the wireless network name (SSID).

```
no guest-mode
```

Disables broadcast of the wireless network name (SSID).

max-association

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`max-association <stations>`

Sets the maximum number of clients stations that can associate with this VAP (VSC).

<stations>	Number of client stations. Range: 1 - 255.

ssid name

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`ssid name <name>`

Specifies the WLAN name (SSID) for the profile.

vlan

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`vlan <id>`

Assigns a VLAN ID to this VAP (VSC).

`no vlan`

Deletes the VLAN ID for this VAP (VSC).

Parameters

<id>	VLAN ID. Range: 1 - 4094.

encryption key 1

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`encryption key <key> <value>`

Sets WEP key 1.

`no encryption key <key>`

Deletes WEP key 1.

Parameters

<key>	WEP key number. Range: 1 - 4. Keys 2 to 4 are only supported on the first WLAN profile.
<value>	Key value. The number of characters you specify for a key determines the level of encryption the service controller will provide. For 40-bit encryption, specify 5 ASCII characters or 10 HEX digits. For 128-bit encryption, specify 13 ASCII characters or 26 HEX digits.

encryption key format

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`encryption key format (hex | ascii)`

Specify the WEP key format.

Parameters

`hex`	Hex keys should only include the following digits: 0-9, a-f, A-F

`ascii`	ASCII keys are much weaker than carefully chosen hex keys. You can include ASCII characters between 32 and 126, inclusive, in the key. However, note that not all client stations support non-alphanumeric characters such as spaces, punctuation, or special symbols in the key.

transmit key

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`transmit key <key number>`

Sets the key the service controller will use to encrypt transmitted data. All four keys are used to decrypt received data.

Parameters

<key number>	Transmit key number. Range: 1 -4.

authentication server access controller

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`authentication server access controller`

Use the access controller to authenticate 802.1X or WPA logins.

authentication server accounting

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`authentication server accounting`

Enables RADIUS accounting for this VAP (VSC).

`no authentication server accounting`

Disables RADIUS accounting for this VAP (VSC).

authentication server accounting radius profile

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`authentication server accounting radius profile <name>`

Sets RADIUS accounting to use the specified RADIUS profile.

`no authentication server accounting radius profile`

Removes accounting support for 802.1x.

authentication server radius

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`authentication server radius <name>`

Sets the RADIUS profile to use for 802.1X or WPA authentication.

dot1x authentication

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`dot1x authentication (local | radius | active-directory)`

Sets the authentication for 802.1X and WPA.

wpa-psk

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`wpa-psk <key>`

Sets the WPA preshared key.

`no wpa-psk`

Deletes the WPA preshared key.

Parameters

<key>	Specify a key that is between 8 and 63 alphanumeric characters in length. It is recommended that the preshared key be at least 20 characters long, and be a mix of letters and numbers. The double quote character should not be used

Description

The service controller uses the key you specify to generate the TKIP keys that encrypt the wireless data stream. Since this is a static key, it is not as secure as the RADIUS option.

authentication server request radius cui

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`authentication server request radius cui`

Include in the authentication request a request for a CUI.

dot1x session page

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`dot1x session page`

IEEE802dot1x authenticated users will be presented with the Session page and the Welcome page after a successful authentication.

`no dot1x session page`

IEEE802dot1x authenticated users will NOT be presented with the Session page and the Welcome page after a successful authentication.

wireless filters

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`wireless filters`

Enables the wireless security filters which only allow traffic to flow between the service controller and a specific upstream device (such as a service controller).

`no wireless filters`

Do not limit traffic flow between the service controller and an upstream device.

This prevents wireless users from accessing resources on the backbone LAN that interconnects the service controller and the upstream device.

wireless filters mac

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`wireless filters mac <mac>`

Sets the MAC address of the upstream device to send traffic to.

`no wireless filters mac <mac>`

Deletes the MAC address of the upstream device to send traffic to.

wireless filters rule input

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`wireless filters rule input <rule>`

Adds a custom filter definition for incoming wireless traffic.

Use this command to define custom security filters for incoming wireless traffic. Filters are specified using standard pcap syntax (http://www.tcpdump.org/tcpdump_man.html) with the addition of a few -specific placeholders. These placeholders can be used to refer to specific MAC addresses and are expanded by the service controller when the filter is activated. Once expanded, the filter must respect the pcap syntax. The pcap syntax is documented in the tcpdump man page:

Placeholders

- %a - MAC address of the access controller.
- %b - MAC address of the bridge.
- %g - Mac address of the default gateway assigned to the service controller.
- %w - MAC address of wireless port.

wireless filters rule output

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`wireless filters rule output <rule>`

Adds a custom filter definition for outgoing wireless traffic.

Use this command to define custom security filters for outgoing wireless traffic. Filters are specified using standard pcap syntax (http://www.tcpdump.org/tcpdump_man.html) with the addition of a few -specific placeholders. These placeholders can be used to refer to specific MAC addresses and are expanded by the service controller when the filter is activated. Once expanded, the filter must respect the pcap syntax. The pcap syntax is documented in the tcpdump man page:

Placeholders

- %a - MAC address of the access controller.
- %b - MAC address of the bridge.
- %g - Mac address of the default gateway assigned to the service controller.
- %w - MAC address of wireless port.

wireless filters type

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
wireless filters type (mac | gateway | rules)
```

Sets the type of wireless security filter to use.

Parameters

`mac`	Traffic is forwarded to an upstream device with a specific MAC address. Wireless security filters use the default definitions.
`gateway`	Traffic is forwarded to the default gateway assigned to the service controller. Wireless security filters use the default definitions.
`custom`	Lets you define custom security filters and address for the upstream device.

Description

The service controller features an intelligent bridge which can apply security filters to safeguard the flow of wireless traffic. The filters limit both incoming and outgoing traffic as defined below, and force the service controller to exchange traffic with a specific upstream device. If the service controller is configured to use the services of a access controller, then the default security filters are automatically enabled and all traffic is sent to the access controller.

Default filters for incoming wireless traffic

Applies to traffic sent from wireless client stations to the AP.

Accepted

- Any IP traffic addressed to the access controller.
- PPPoE traffic (The PPPoe server must be the upstream device.)
- IP broadcast packets, except NetBIOS
- Certain address management protocols (ARP, DHCP) regardless of their source address.
- Any traffic addressed to the AP, including 802.1x.

Blocked

- All other traffic is blocked. This includes NetBIOS traffic regardless of its source/destination address. TTPS traffic not addressed to the AP (or upstream device) is also blocked, which means wireless client stations cannot access the management tool on other products.

Default filters for outgoing wireless traffic

Applies to traffic sent from the AP to wireless client stations.

Accepted

- Any IP traffic coming from the upstream device, except NetBIOS packets.
- PPPoE traffic from the upstream device.
- IP broadcast packets, except NetBIOS
- ARP and DHCP Offer and ACK packets.
- Any traffic coming from the AP itself, including 802.1x.

Blocked

- All other traffic is blocked. This includes NetBIOS traffic regardless of its source/destination address.

mac authentication accounting

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`mac authentication accounting`

Enables RADIUS accounting for this VAP (VSC).

`no mac authentication accounting`

Disables RADIUS accounting for this VAP (VSC).

mac authentication accounting radius profile

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`mac authentication accounting radius profile <name>`

Sets RADIUS accounting to use the specified RADIUS profile.

`no mac authentication accounting radius profile`

Disables accounting support for MAC authentication.

mandatory authentication

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`mandatory authentication`

MAC-based authentication is mandatory.

`no mandatory authentication`

MAC-based authentication is not mandatory.

mac authentication radius profile

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`mac authentication radius profile <radiusname>`

Specifies the name of the RADIUS profile to use for MAC-based authentication.

`no mac authentication radius profile`

Do not use a RADIUS profile.

mac authentication remote

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`mac authentication remote`

Sets MAC-based authentication to use a RADIUS profile.

`no mac authentication remote`

MAC-based authentication will not use a RADIUS profile.

mac authentication request radius cui

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`mac authentication request radius cui`

Include a request for a CUI in authentication requests.

mac authentication local

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
mac authentication local
```

Sets MAC-based authentication to use the local user list to validate the MAC addresses of client stations.

```
no mac authentication local
```

Do not use the local user list for MAC-based authentication.

mac authentication

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
mac authentication
```

Enables support for MAC-based authentication.

```
no mac authentication
```

Disable support for MAC-based authentication.

html authentication

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
html authentication
```

Enables HTML authentication.

```
no html authentication
```

Disables HTML authentication.

html authentication accounting

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
html authentication accounting
```

Enables RADIUS accounting.

```
no html authentication accounting
```

Disables RADIUS accounting.

html authentication accounting radius profile

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
html authentication accounting radius profile <name>
```

Sets RADIUS accounting for HTML users to use the specified RADIUS profile.

```
no html authentication accounting radius profile
```

Disables RADIUS accounting RADIUS support for HTML users.

html authentication active-directory

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
html authentication active-directory
```

Use Active Directory (AD) to authenticate users.

```
no html authentication active-directory
```

Do not use Active Directory (AD) to authenticate users.

html authentication local

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
html authentication local
```

Validate HTML logins using the local user list.

```
no html authentication local
```

Do not validate HTML logins using the local user list.

html authentication radius

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
html authentication radius
```

Validate HTML logins using the specified RADIUS profile.

```
no html authentication radius
```

Do not validate HTML logins using the specified RADIUS profile.

html authentication radius profile

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
html authentication radius profile <name>
```

Validate HTML logins using the specified RADIUS profile.

```
no html authentication radius profile
```

Do not validate HTML logins using the specified RADIUS profile.

html authentication request radius cui

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
html authentication request radius cui
```

Include a request for a CUI in the authentication request.

```
no html authentication request radius cui
```

Do not include a request for a CUI in the authentication request.

html authentication timeout

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
html authentication timeout <number>
```

Sets the HTML authentication timeout.

active

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`active`

Enable this VAP (VSC).

`no active`

Disable this VAP (VSC).

beacon dtim count

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`beacon dtim count <number>`

Defines the DTIM period in the beacon.

Client stations use the DTIM to wake up from low-power mode to receive multicast traffic. The service controller transmits a beacon every 100 ms. The DTIM counts down with each beacon that is sent, therefore if the DTIM is set to 5, then client stations in low-power mode will wake up every 500 ms (.5 second) to receive multicast traffic.

beacon transmit power

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`beacon transmit power`

Advertise the current transmit power setting in the beacon.

`no beacon transmit power`

Do not advertise the current transmit power setting in the beacon.

data rate

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`data rate (a | b | g | bg | n) <rate>`

Enable the given data rate for a particular PHY type.

`no data rate (a | b | g | bg | n) <rate>`

Disable the given data rate for a particular PHY type.

public forwarding

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`public forwarding (any | 802.1x | none | ipv6)`

Enables support for traffic exchange between wireless client stations.

access lan stations

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`access lan stations`

Permits traffic exchange between wireless and LAN stations.

```
no access lan stations
```

Blocks traffic exchange between wireless and LAN stations.

fast authentication

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
fast authentication
```

Enables WPA2 opportunistic key caching.

```
no fast authentication
```

Disables WPA2 opportunistic key caching.

layer3 mobility

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
layer3 mobility
```

Enables Layer 3 mobility.

```
no layer3 mobility
```

Disables Layer 3 mobility.

add ip-qos profile

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
add ip-qos profile  <name>
```

Adds the specified profile to the list of IP QoS profiles in effect for this VAP (VSC).

<profile-name> Name of an existing IP QoS profile.

delete ip-qos profile all

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
delete ip-qos profile all
```

Clears the list of IP QoS profiles currently in effect for this VAP (VSC).

delete ip-qos profile

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
delete ip-qos profile <name>
```

Removes the specified profile from the list of IP QoS profiles in effect for this VAP (VSC).

<profile-name> Name of an existing IP QoS profile currently in the profile list for this VAP (VSC).

qos

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
qos ( 802.1p | very-high | high | normal | low | diffsrv | tos | default | vap0
| vap1 | vap2 | vap3)
```

Sets the QoS level for this profile.

`no qos`

Disables QoS for this profile.

Four traffic queues are provided based on the WME standard. In order of priority, these queues are:

- 1: Voice traffic
- 2: Video traffic
- 3: Best effort data traffic
- 4: Background data traffic

Each QoS priority mechanism maps traffic to one of the four traffic queues. Client stations that do not support the QoS mechanism for the profile they are connected to are always assigned to queue 3.

Important: Traffic delivery is based on strict priority (per the WME standard). Therefore, if excessive traffic is present on queues 1 or 2, it will reduce the flow of traffic on queues 3 and 4.

`802.1p`	Traffic from 802.1p client stations is classified based on the VLAN priority field present within the VLAN header. When this mechanism is selected, the service controller will advertise WME capabilities, enabling WME clients to associate and take advantage of them. This setting has no effect on legacy clients. Note: To support 802.1p, the wireless profile must have a VLAN assigned to it, which means that client station traffic is forwarded onto the LAN port only.
`vap0 to vap3`	Allows a specific priority level to be specified for all traffic on a VAP (VSC) profile. This enables client stations without a QoS mechanism to set traffic priority by connecting to the appropriate SSID. If you enable this priority mechanism, it takes precedence regardless of the priority mechanism supported by associated client stations. For example, if you set SSID-based low priority for a profile, all devices that connect to the profile have their traffic set at this priority Mapping to the traffic queues is as follows: vap0 or very-high=queue 1, vap1 or high=queue 2, vap2 or normal=queue 3, vap3 or low=queue 4
`diffsrv`	Differential services is a method for defining IP traffic priority on a per-hop basis. The Differential Service bits are defined in RFC2474 and are composed of the six most significant bits of the IP TOS field. These bits define the class selector code points which the CN320 maps to the appropriate traffic queue. (default setting)
`tos`	The IP TOS (type of service) field can be used to mark prioritization or special handling for IP packets.

upstream diffserv tagging

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`upstream diffserv tagging`

Enables upstream diffserv tagging.

`no upstream diffserv tagging`

Disables upstream diffserv tagging.

wmm advertising

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`wmm advertising`

Enables WMM information element advertising.

`no wmm advertising`

Disables WMM information element advertising.

html redirection

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`html redirection`

Enables support for HTML logins.

`no html redirection`

Disables support for HTML logins.

local nas id

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`local nas id <nasid>`

Set the NAS Id when only local authentication is configured.

`use local nas id`

Enables the use of NAS Id when only local authentication is configured.

`no use local nas id`

Disables the use of NAS Id when only local authentication is configured.

bandwidth

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`bandwidth (very-high | high | normal | low)`

Sets the bandwidth level.

bandwidth default rates

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`bandwidth default rates`

Enables default bandwidth rates for this VAP (VSC).

`no bandwidth default rates`

Disables default bandwidth rates for this VAP (VSC).

bandwidth default rates maximum

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`bandwidth default rates maximum <max-tx-rate> <max-rx-rate>`

Sets the default maximum transmit and receive rates.

radius accounting realms

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`radius accounting realms`

Use RADIUS accounting realms.

`no radius accounting realms`

Do not use RADIUS accounting realms.

radius authentication realms

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`radius authentication realms`

Use RADIUS authentication realms.

`no radius authentication realms`

Do not use RADIUS authentication realms.

identify stations by ip only

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`identify stations by ip only`

Identify stations based on IP address only.

`no identify stations by ip only`

Do not identify stations based on address IP only.

location-aware group

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`location-aware group <name>`

Sets the specified group name for the access point.

`no location-aware group`

Deletes the specified group name for the access point.

location-aware called-station-id content

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`location-aware called-station-id content (ssid | group | mac)`

Sets the value returned in Called-Station-ID.

dhcp relay

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`dhcp relay <primary-ip-address> <[secondary-ip-address]>`

Sets the primary and secondary DHCP server for the relay.

`no dhcp relay`

Resets the primary and secondary DHCP server for the relay.

dhcp relay active

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`dhcp relay active`

The dhcp relay is enabled on the VAP (VSC).

`no dhcp relay active`

The dhcp relay is not enabled on the VAP (VSC).

dhcp relay circuit id

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`dhcp relay circuit id <string>`

Sets the Option 82 circuit ID.

`no dhcp relay circuit id`

Clears the Option 82 circuit ID.

dhcp relay remote id

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`dhcp relay remote id <string>`

Sets the Option 82 remote ID.

`no dhcp relay remote id`

Clears the Option 82 remote ID.

dhcp relay subnet

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`dhcp relay subnet <ip address>/<mask>`

Sets the DHCP relay subnet.

`no dhcp relay subnet`

Clears the DHCP relay subnet.

dhcp server

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`dhcp server`

The dhcp server is enabled on the VAP (VSC).

`no dhcp server`

The dhcp server is not enabled on the VAP (VSC).

dhcp server dns

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`dhcp server dns <ip address>`

Sets the domain name server provided to DHCP clients.

```
no dhcp server dns
```

Reset the domain name server provided to DHCP clients.

dhcp server gateway

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
dhcp server gateway <ip address>
```

Sets the default gateway provided to DHCP clients.

```
no dhcp server gateway
```

Reset the default gateway provided to DHCP clients.

dhcp server range

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
dhcp server range <start-range> <end-range>
```

Specify the DHCP server IP address range.

dhcp server subnet

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
dhcp server subnet <ip address>/<mask>
```

Sets the DHCP server subnet.

```
no dhcp server subnet
```

Clears the DHCP server subnet.

radius-framed-protocol-attribute

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
radius-framed-protocol-attribute
```

Include the RADIUS Framed-Protocol attribute in Access Request packets. The value for this attribute is PPP (1).

```
no radius-framed-protocol-attribute
```

Do not include the RADIUS Framed-Protocol attribute in Access Request packets.

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
end
```

Switches to parent context.

security

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
security (none | wep | 802.1x [wep | static-wep] | wpa (psk | radius) [ v1 | v2
] )
```

Sets the current wireless security policy.

Parameters

`none`	No wireless security.
`wep`	This option enables support for wireless users with WEP client software.
`802.1x`	This option enables support for wireless users with 802.1X client software. The service controller supports 802.1x client software that uses EAP-TLS, EAP-TTLS, EAP-SIM, and PEAP.
`wep`	Enables the use of dynamic WEP keys for all 802.1X sessions. Dynamic key rotation occurs on key 1, which is the broadcast key. Key 0 is the pairwise key. It is automatically generated by the service controller.
`static-wep`	Support client stations using static WEP keys.
`wpa`	This option enables support for wireless users with WPA client software.
`psk`	Enables support for a preshared key:
`radius`	The service controller obtains the MPPE key from the RADIUS server. This is a dynamic key that changes each time the user logs in and is authenticated. The MPPE key is used to generate the TKIP keys that encrypt the wireless data stream.
`v1,v2`	Specify which version of WPA to use. None will use both versions (mixed mode).

VLAN interface context

Path: View > Enable > Config > Internet interface > VLAN interface
View > Enable > Config > LAN interface > VLAN interface

This context provides commands for configuring Virtual LANs (VLANs). In this context, VLANs can be added or edited.

For example, to create a new VLAN interface named "hongkong" on the LAN port with VLAN id 88, do the following:

CLI(config)# interface lan

CLI(if-lan)# interface vlan 88

CLI(if-vlan)# vlan name hongkong

CLI(if-vlan)# ip address mode dhcp

CLI(if-vlan)# no nat

CLI(if-vlan)# end

CLI(if-lan)#

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`end`

Switches to parent context.

ip address

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`ip address <ip address>/<mask>`

Sets a static IP address for the VLAN.

Parameters

<address>	IP address.
</mask>	Subnet mask in CIDR format. Specifies the number of bits in the mask.

ip address mode

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`ip address mode (dhcp | static | none)`

Sets the IP addressing mode for this VLAN interface.

Parameters

`dhcp`	Dynamic host configuration protocol. The DHCP server will automatically assign an address to the service controller, which functions as a DHCP client.
`static`	This option enables you to manually assign an IP address to the service controller.
`none`	This VLAN does not have an IP address.

vlan name

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`vlan name <name>`

Change the name of this VLAN interface.

ip default-gateway

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`ip default-gateway <ip address>`

Sets the default gateway for this VLAN.

`no ip default-gateway`

Removes the default gateway for this VLAN.

ip nat

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`ip nat`

Enable Network Address translation for this interface.

`no ip nat`

Disable Network Address translation for this interface.

RADIUS context

Path: View > Enable > Config > RADIUS

This context provides commands for configuring RADIUS profiles.

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
end
```

Switches to parent context.

radius-server accounting port

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
radius-server accounting port <number>
```

Specifies the port to use for RADIUS accounting.

Parameters

<number>	Accounting port number. Range: 1 - 65535.

radius-server alternate hosts

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
radius-server alternate hosts
```

Try last answering RADIUS host first.

```
no radius-server alternate hosts
```

Try primary RADIUS host first.

radius-server authentication method

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
radius-server authentication method (mschap | chap | mschapv2 | pap | eap-md5)
```

Sets the authentication method to use when communicating with the RADIUS server.

For 802.1x users, the authentication method is always determined by the 802.1x client software and is not controlled by this setting.

If traffic between the service controller and the RADIUS server is not protected by a VPN, it is recommended that you use either EAP-MD5 or MSCHAP V2, if supported by your RADIUS Server. (PAP, MSCHAP V1 and CHAP are less secure protocols.)

radius-server authentication port

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
radius-server authentication port <number>
```

Specifies the port to use for RADIUS authentication. By default, RADIUS servers use port 1812.

Parameters

<number>	Authentication port number. Range: 1 - 65535

radius-server deadtime

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`radius-server deadtime <seconds>`

Sets the retry interval for access and accounting requests that time-out.

If no reply is received within this interval, the service controller switches between the primary and secondary RADIUS servers (if defined). If a reply is received after the interval expires, it is ignored.

Parameters

<seconds>	Retry interval. Range: 2 - 60 seconds.

radius-server host

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`radius-server host <primary>[<secondary>]`

Sets the addresses of the primary and secondary RADIUS servers.

Parameters

<primary>	IP address of the primary RADIUS server.
<secondary>	IP address of the secondary RADIUS server.

radius-server key 2

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`radius-server key <primary>[<secondary>]`

Enter primary and secondary secrets.

Parameters

<primary>	Shared secret for the primary RADIUS server.
<secondary>	Shared secret for the secondary RADIUS server.

radius-server message-authenticator

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`radius-server message-authenticator`

Include the message authenticator attribute in RADIUS packets.

`no radius-server message-authenticator`

Do not include the message authenticator attribute in RADIUS packets.

radius-server name

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`radius-server name <name>`

Changes the name of the RADIUS profile.

radius-server nasid

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`radius-server nasid <id>`

Sets the network access server ID you want to use for the service controller.

By default, the serial number of the service controller is used. The service controller includes the NAS-ID attribute in all packets that it sends to the RADIUS server.

radius-server timeout

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`radius-server timeout`

Activates RADIUS timeout.

`no radius-server timeout`

Disables RADIUS timeout.

radius-server timeout

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`radius-server timeout <number>`

Sets the total timeout for RADIUS requests.

`no radius-server timeout`

Disables RADIUS timeout.

radius-server force-nas-port-to-vlanid

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`radius-server force-nas-port-to-vlanid`

Force the NAS-Port attribute to ingress VLAN ID in RADIUS packets.

`no radius-server force-nas-port-to-vlanid`

Do not force the NAS-Port attribute to ingress VLAN ID in RADIUS packets.

radius-server realm

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`radius-server realm (regex | text)`

Specifies if realms in list are regular expressions or just plain text.

radius-server realm name

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`radius-server realm name <name>`

Adds the specified realm name.

`no radius-server realm name <name>`

Removes the specified realm name.

DHCP server context

Path: View > Enable > Config > DHCP server

This context lets you configure DHCP server settings.

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`end`

Switches to parent context.

active

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`active`

This range is enabled.

`no active`

This range is not enabled.

gateway

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`gateway <ip address>`

Sets the default gateway provided to DHCP clients.

`no gateway`

Reset the default gateway provided to DHCP clients.

range

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`range <start-range> <end-range>`

Specify the DHCP server IP address range.

permanent leases

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`permanent leases <ip address> <macaddr> <uid>`

Adds a permanent DHCP lease for this mapping.

`no permanent leases <ip address> <macaddr> <uid>`

Deletes a permanent DHCP lease for this mapping.

GRE interface context

Path: View > Enable > Config > GRE interface

Details of the GRE interface.

end force

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`end [force]`

Quits the GRE context.

gre name

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`gre name <name>`

Renames the current GRE interface.

ip address

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`ip address <ip address>/<mask>`

Set the local tunnel IP address and mask.

peer ip address

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`peer ip address <ip address>`

Sets the GRE peer IP address.

remote ip address

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`remote ip address <ip address>`

Sets the remote tunnel IP address.

IPsec policy context

Path: View > Enable > Config > IPsec policy

This context allows editing of IPSec configuration settings.

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
end
```

Switches to parent context.

active

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
active
```

Enables policy.

```
no active
```

Disables policy.

authentication

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
authentication (x509 | psk)
```

Selects between x509 and psk authentication.

cipher

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
cipher aes
```

Sets the desired encryption algorithm.

```
no cipher aes
```

Do not use this encryption algorithm.

dns domain

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
dns domain <names>
```

Sets the domain name for this policy.

```
no dns domain <names>
```

Resets the domain name for this policy.

dns server

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
dns server ( <ip address> | none )
```

Sets the DNS server for this policy.

```
no dns server
```

Resets the DNS server for this policy.

incoming nat

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
incoming nat
```

Enables NAT for incoming traffic.

```
no incoming nat
```

Disables NAT for incoming traffic.

incoming traffic network

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
incoming traffic network <ip address>/<mask>
```

Sets the Phase 2 incoming network.

interface

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
interface (lan | internet)
```

Sets the interface this policy applies to.

local id

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
local id (ip-address <ip address> | host <name> | email <address> | dn <dn>)
```

Specify the local id type and value.

mode

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
mode (main | aggressive) (tunnel | transport)
```

Sets the IPSec mode.

outgoing traffic network

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
outgoing traffic network <ip address>/<mask>
```

Sets the Phase 2 outgoing network.

peer id

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
peer id (ip-address <ip address> | host <name> | email <address> | dn <dn>)
```

Specify the peer id type and value.

peer ip address

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`peer ip address (<ip address>| any )`

Set the peer ip address for this policy.

perfect forward secrecy

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`perfect forward secrecy`

Enable PFS.

`no perfect forward secrecy`

Disable PFS.

preshared key

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`preshared key <secret>`

Sets the preshared key.

`no preshared key`

Removes the preshared key.

Syslog destination context

Path: View > Enable > Config > Syslog destination

This context provides commands for configuring Syslog destinations.

active

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
active
```

Enables logging to the current destination.

```
no active
```

Disables logging to the current destination.

logging facility

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
logging facility (local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7)
```

Sets the facility that is used when logging messages to a syslog server.

Parameters

<facility>	Available facilities are: local0 - local7.

logging host

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
logging host (tcp | udp) <addr> [<number>]
```

Sets the remote address, the connection protocol and port of current syslog remote destination.

logging prefix

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
logging prefix <string>
```

Sets the prefix that will be prepended to all syslog messages.

```
no logging prefix
```

Removes the prefix that is prepended to all syslog messages.

name

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
name <name>
```

Renames the current syslog destination.

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
end
```

Switches to parent context.

level

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
level
```

Enables filtering of the log file by severity level.

```
no level
```

Disables filtering of the log file by severity level.

level

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
level (lower | higher) (debug | info | notice | warning | error | critical |
alert | emergency)
```

Defines the severity of messages that will be logged.

```
no level
```

Disables filtering of the log file by severity level.

Parameters

`debug`	Debug-level messages.
`info`	Informational messages.
`notice`	Normal, but significant condition.
`warning`	Warning conditions.
`error`	Error conditions.
`critical`	Critical conditions.
`alert`	Action must be taken immediately.
`emergency`	System is unusable.

matches

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
matches (any | all) filters
```

All three log file filters (message, process, and level) are combined to filter the log according to this setting.

message

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
message
```

Enables filtering of the log file message field.

```
no message
```

Disables filtering of the log file message field.

message

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
message (matches | notmatches) <regex>
```

Use this filter to include log messages. Use a regular expression to define the match criteria for the log file message field.

```
no message
```

Disables filtering of the log file message field.

process

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
process
```

Enables filtering of the log file by process name.

```
no process
```

Disables filtering of the log file by process name.

process

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
process (matches | notmatches) <string>
```

Use this filter to include log messages according to their process name.

```
no process
```

Disables filtering of the log file by process name.

PPTP client interface context

Path: View > Enable > Config > PPTP client interface

This is the PPTP client context.

active

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
active
```

Sets PPTP client connection to 'up'.

```
no active
```

Sets PPTP client connection to 'down'.

pptp client credentials

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
pptp client credentials <name> <password>
```

Sets the PPTP username and password.

pptp client domain name

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
pptp client domain name <name>
```

Sets the domain name used by the PPTP client.

pptp client server address

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
pptp client server address <address>
```

Sets the IP address to connect to.

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
end
```

Switches to parent context.

ip nat

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
ip nat
```

Enables NAT for the PPTP client.

```
no ip nat
```

Disables NAT for the PPTP client.

pptp client auto route discovery

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
pptp client auto route discovery
```

Enables auto-route discovery.

```
no pptp client auto route discovery
```

Disables auto-route discovery.

pptp client lcp echo

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
pptp client lcp echo
```

Enables PPTP LCP echo.

```
no pptp client lcp echo
```

Disables PPTP LCP echo.

passive-interface

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
passive-interface
```

Only listen to RIP, never send.

```
no passive-interface
```

Send and listen for RIP.

router rip

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
router rip
```

Enables RIP for this interface.

```
no router rip
```

Disables RIP on this interface.

Keychain context

Path: View > Enable > Config > Keychain

Manage a keychain: a collection of keys.

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`end`

End current context.

key

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`key <number>`

Enter new key.

`no key <number>`

Delete key with given ID.

key chain name

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`key chain name <name>`

Rename current keychain.

Keys context

Path: View > Enable > Config > Keychain > Keys

Edit a key, as part of a keychain.

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
end
```

End current context.

key-string

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
key-string <name>
```

Set the authentication string for this key.

```
no key-string
```

Remove the authentication string for this key.

Subscription plan context

Path: View > Enable > Config > Subscription plan

Details about a subscription plan.

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`end`

End current context.

daily restriction

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`daily restriction <from> <to>`

Sets the daily restrictions hours.

`use daily restriction`

Enable daily restrictions.

`no use daily restriction`

Disable daily restrictions.

end time

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`end time <datetime>`

Set the account end date and time. "YYYY-MM-DD HH:MM:SS".

`use end time`

Use account end time.

`no use end time`

Do not use account end time.

initial login time allocation

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`initial login time allocation <number> (minutes | hours | days)`

Sets the amount of time allocated after the first login by a user.

`use initial login time allocation`

Use the initial login time allocation.

`no use initial login time allocation`

Do not use the initial login time allocation.

online time limit

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`online time limit`

Use the online time limit.

`no online time limit`

Do not use the online time limit.

online time limit

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`online time limit <number> (minutes | hours | days)`

Sets the initial online time for an account.

`no online time limit`

Do not use the online time limit.

start time

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`start time <datetime>`

Set the account start date and time. "YYYY-MM-DD HH:MM:SS".

`use start time`

Use account start time.

`no use start time`

Do not use account start time.

subscription plan name

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`subscription plan name <newname>`

Change the subscription plan name.

public ip reservation

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`public ip reservation`

Enables public IP address reservation.

`no public ip reservation`

Disables public IP address reservation.

public ip subnet

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`public ip subnet`

Set profile to use the public IP subnet for IP Addressing once authenticated.

`no public ip subnet`

Removes this attribute.

`use public ip subnet`

Use this attribute.

`no use public ip subnet`

Do not use this attribute.

SNMP user context

Path: View > Enable > Config > SNMP user

This context provides commands for configuring SNMP user.

access level

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`access level (read-only | read-write)`

Specifies the access level for this SNMP user.

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`end`

Returns to a previous context.

password

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`password <password>`

Specifies the password for this SNMP user.

security

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`security (md5-des | sha-aes)`

Specifies the security for this SNMP user.

user name

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`user name <name>`

Changes the name of this SNMP user.

SNMP notification receiver context

Path: View > Enable > Config > SNMP notification receiver

This context provides commands for configuring SNMP notification receiver.

community

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`community <community>`

Specifies the community for this SNMP notification receiver.

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`end`

Returns to a previous context.

port

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`port <number>`

Specifies the UDP port for this SNMP notification receiver.

receiver

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`receiver <host>`

Changes the host name of the SNMP notification receiver.

user

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`user <name>`

Specifies the user for this SNMP notification receiver.

version

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`version (1 | 2c | 3)`

Specifies the SNMP version for this SNMP notification receiver.

Active Directory Group context

Path: View > Enable > Config > Active Directory Group

Contains information about attributes to send when a user is related to an Active Directory group.

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
end
```

Switches to parent context.

access controlled

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
access controlled
```

Make this user access controlled.

```
no access controlled
```

Make this user not access controlled.

access-controlled profile

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
access-controlled profile <name>
```

Use this session profile for this account.

```
no access-controlled profile <name>
```

Do not use this session profile for this account.

```
use access-controlled profile
```

Use the Access Controlled profiles.

```
no use access-controlled profile
```

Do not use the Access Controlled profiles.

access-controlled virtual ap

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
access-controlled virtual ap <name>
```

Add to the list of allowed virtual APs.

```
no access-controlled virtual ap <name>
```

Remove from the list of allowed virtual APs.

```
use access-controlled virtual ap
```

Use only allowed Virtual APs (VSCs) for this profile.

```
no use access-controlled virtual ap
```

Use any Virtual APs (VSCs) for this profile.

active

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`active`

Enable this user account.

`no active`

Disable this user account.

active-directory group name

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`active-directory group name <name>`

Change the name for this user.

egress vlan

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`egress vlan <number>`

Set the VLAN tunnel ID.

`use egress vlan`

Use the VLAN tunnel ID.

`no use egress vlan`

Do not use the VLAN tunnel ID.

regular profile

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`regular profile <name>`

Apply a non-access-controlled profile.

`no regular profile <name>`

Remove a non-access-controlled profile.

`use regular profile`

Use the non-access controlled profiles.

`no use regular profile`

Do not use the non-access controlled profiles.

regular virtual ap

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`regular virtual ap <name>`

Add to the list of allowed virtual APs (VSCs).

`no regular virtual ap <name>`

Remove from the list of allowed virtual APs (VSCs).

```
use regular virtual ap
```

Use only allowed Virtual APs (VSCs) for this profile.

```
no use regular virtual ap
```

Use any Virtual AP (VSC) for this profile.

Controlled Network AP context

Path: View > Enable > Controlled Network AP

Contains commands for controlled network AP configuration.

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
end
```

Switches to parent context.

execute action

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
execute action (synchronize | accept-suspicious | accept-product | rediscover)
```

Execute an action on the entity's devices.

execute system action

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
execute system action (restart | reset | switch-mode)
```

Execute a system action on the AP.

show config factory

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
show config [factory]
```

Displays the current configuration as a list of CLI commands.

ap group

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
ap group <name>
```

Change the AP group (must Synchronize).

ap name

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
ap name <name>
```

Change the current AP name.

config

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
config
```

Switch to generic configuration context.

contact

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`contact <name>`

Modify the contact.

location

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`location <name>`

Modify the location.

product type

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`product type (map-320 | map-330 | map-625 | map-630 | msm410 | msm317 )`

Set the product type of the AP that you are about to pre-configure. Some legacy product names are still used. They correspond to HP ProCurve Networking product names as follows:

Name in syntax	Corresponding Hp ProCurve name
`map-320`	MSM310
`map-330`	MSM320, MSM325 (with sensor license)
`map-625`	MSM422
`map-630`	MSM335

Controlled Network AP Group context

Path: View > Enable > Controlled Network AP Group

Contains commands for controlled network AP Group configuration.

execute action

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`execute action (synchronize | accept-suspicious | accept-product | rediscover)`

Execute an action on the entity's devices.

show config factory

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`show config [factory]`

Displays the current configuration as a list of CLI commands.

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`end`

Switch to parent context.

config

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`config`

Switch to generic configuration context.

group name

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`group name <name>`

Change the current group name.

virtual ap binding

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`virtual ap binding <vapprofile>`

Create/use a VAP (VSC) binding.

`no virtual ap binding <vapprofile>`

Delete a VAP (VSC) binding.

Controlled Network Base Group context

Path: View > Enable > Controlled Network Base Group

Contains commands for controlled network Base Group configuration.

execute action

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
execute action (synchronize | accept-suspicious | accept-product | rediscover)
```

Execute an action on the entity's devices.

show config factory

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
show config [factory]
```

Displays the current configuration as a list of CLI commands.

config

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
config
```

Switch to generic configuration context.

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
end
```

Switch to parent context.

Controlled Network context

Path: View > Enable > Controlled Network AP > Controlled Network
View > Enable > Controlled Network AP Group > Controlled Network
View > Enable > Controlled Network Base Group > Controlled Network

Contains commands for controlled network configuration.

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
end
```

interface wireless

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
interface wireless <number> [<product>]
```

Switch to the wireless interface context.

local mesh group

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
local mesh group <group>
```

Switch to local mesh group context.

local mesh provisioning group

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
local mesh provisioning group
```

Switch to local mesh provisioning group context.

provisioning connectivity

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
provisioning connectivity
```

Switch to provisioning connectivity context.

provisioning discovery

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
provisioning discovery
```

Switch to provisioning discovery context.

radius profile

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
radius profile <profile>
```

Switch to controlled network radius profile context.

switch port

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`switch port <name>`

Switch to the ethernet port context.

syslog

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`syslog`

Switch to syslog context.

sensor server name

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`sensor server name <name>`

Sets the IP address or hostname of the the RF Manager Server to connect to.

Parameters

`Name`	Specify the IP address of the the RF Manager Server or its hostname. If a hostname is specified, the service controller must be able to resolve it via DNS, that is, an entry must be created on the network DNS server that points to the IP address of the RF Manager Server.

sensor server id

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`sensor server id <id>`

Sets the server ID of the the RF Manager Server to connect to.

Parameters

`ID`	Specify the Server ID of the RF Manager Server to connect to. Set the Server ID to 0 to have the service controller send a discovery request to all active RF Manager Servers. The service controller will connect to the first server that responds to the discovery request.

sensor discovery mode

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`sensor discovery mode (id | ip)`

Sets the method the service controller will use to communicate with the RF Manager Server.

Parameters

`id`	Connect using the Server ID of the RF Manager Server.
`ip`	Connect using the IP address or hostname of the RF Manager Server.

Description

For these methods to work, the following must be true:

- The service controller must be able to reach the RF Manager Server via a network connected to port 1 or port 2. For example, you should be able to ping the RF Manager Server IP address from the service controller.

- If there are any firewalls between the service controller and the RF Manager Server, then TCP and UDP ports 3851 must be open bidirectionally.
- If using the hostname option, an entry must be created on the network DNS server that points to the IP address of the RF Manager Server.
- If using the Server ID option, support for multicast traffic must be enabled on all routers and switches connected between the service controller and the RF Manager Server.

sensor network detector

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
sensor network detector
```

Enable the Network Detector.

```
no sensor network detector
```

Disable the Network Detector.

inherit sensor

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
inherit sensor
```

Inherit sensor settings from parent.

```
no inherit sensor
```

Do not inherit sensor settings from parent.

dynamic key

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
dynamic key
```

Enables dynamic key support for 802.1X and WPA.

```
no dynamic key
```

Disables dynamic key support for 802.1X and WPA.

dynamic key interval

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
dynamic key interval (5m | 10m | 15m | 30m | 1h | 2h | 4h | 8h | 12h)
```

Specifies how often (in minutes or hours) that the group (broadcast) key is changed for 802.1X and WPA.

dot1x reauth

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
dot1x reauth
```

Enable this option to force 802.1X client stations to reauthenticate.

```
no dot1x reauth
```

Disables 802.1X reauthentication.

dot1x reauth period

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
dot1x reauth period (15m | 30m | 1h | 2h | 4h | 8h | 12h)
```

Sets the 802.1X reauthentication interval. Client stations must reauthenticate when this interval expires.

dot1x reauth terminate

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
dot1x reauth terminate
```

Enable this option to allow client stations to remain connected during re-authentication. Client traffic is blocked only when re-authentication fails.

```
no dot1x reauth terminate
```

Disabled this option to block client traffic during re-authentication and only activate traffic again if authentication succeeds.

dot1x supplicant timeout

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
802.1x supplicant time-out <seconds>
```

Sets the 802.1X supplicant time-out.

Parameters

<seconds>	time-out in seconds.

inherit 8021x

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
inherit 802.1x
```

Inherit 802.1x settings from parent.

```
no inherit 802.1x
```

Do not inherit 802.1x settings from parent.

bridge protocol ieee

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
bridge protocol ieee
```

Enable the bridge spanning tree protocol to prevent undesirable loops from occurring in the network that may result in decreased throughput.

```
no bridge protocol ieee
```

Disable the bridge spanning tree protocol.

inherit untagged stp

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
inherit untagged stp
```

Inherit untagged spanning tree protocol settings from parent.

```
no inherit untagged stp
```

Do not inherit untagged spanning tree protocol settings from parent.

bridge protocol ieee vlan

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
bridge protocol ieee vlan
```

Enable the bridge spanning tree protocol for VLANs.

```
no bridge protocol ieee vlan
```

Disable the bridge spanning tree protocol for VLANs.

inherit vlan stp

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
inherit vlan stp
```

Inherit vlan spanning tree protocol settings from parent.

```
no inherit vlan stp
```

Do not inherit vlan spanning tree protocol settings from parent.

inherit local mesh qos

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
inherit local mesh qos
```

Inherit local mesh QoS settings from parent.

```
no inherit local mesh qos
```

Do not inherit local mesh QoS settings from parent.

local mesh ip qos profile

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
local mesh ip qos profile <profile>
```

Add an IP Qos profile to the profile's list.

```
no local mesh ip qos profile <profile>
```

Delete an IP QoS profile from the profile's list.

local mesh qos mechanism

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
local mesh qos mechanism (disabled | 802.1p | very_high | high | normal | low | diffsrv | tos | ip_qos)
```

Set the QoS priority mechanism.

enable vsc services

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
enable vsc services
```

Enable wireless services when the service controller is unreachable.

```
no enable vsc services
```

Shutdown wireless services when the service controller is unreachable.

inherit service availability

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
inherit service availability
```

Inherit service availability from parent.

```
no inherit service availability
```

Do not inherit service availability from parent.

inherit l3subnets

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
inherit l3subnets
```

Inherit L3 subnets from parent.

```
no inherit l3subnets
```

Do not inherit L3 subnets from parent.

l3subnet

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

l3subnet *<vlanid> <ipsubnet> <ipnetmask>*

Add a new l3subnet to the list.

no l3subnet *<vlanid> <ipsubnet> <ipnetmask>*

Delete an l3subnet from the list.

inherit switch ports

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
inherit switch ports
```

Inherit settings from the switch ports.

```
no inherit switch ports
```

Inherit settings from the switch ports.

Virtual AP Binding context

Path: View > Enable > Controlled Network AP Group > Virtual AP Binding

Configuration for VAP Bindings

dual radio binding

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
dual radio binding (radio1 | radio2)
```

Enables radio binding.

```
no dual radio binding (radio1 | radio2)
```

Disables radio binding.

egress vlan

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
egress vlan
```

Enable the egress vlan.

```
no egress vlan
```

Disable the egress vlan.

egress vlan

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
egress vlan <number>
```

Set the egress vlan id.

```
no egress vlan
```

Disable the egress vlan.

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
end
```

Switch to parent context.

location aware

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
location aware <name>
```

Set the location-aware group name.

Syslog context

Path: View > Enable > Controlled Network AP > Controlled Network > Syslog
View > Enable > Controlled Network AP Group > Controlled Network > Syslog
View > Enable > Controlled Network Base Group > Controlled Network > Syslog

Set basic configuration for entity's logging.

message

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`message (matches | notmatches) <regex>`

Use this filter to include log messages. Use a regular expression to define the match criteria for the log file message field.

`no message`

Disables filtering of the log file message field.

message

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`message`

Enables filtering of the log file message field.

`no message`

Disables filtering of the log file message field.

process

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`process (matches | notmatches) <string>`

Use this filter to include log messages according to their process name.

`no process`

Disables filtering of the log file by process name.

process

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`process`

Enables filtering of the log file by process name.

`no process`

Disables filtering of the log file by process name.

level

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`level (lower | higher) (debug | info | notice | warning | error | critical | alert | emergency)`

Defines the severity of messages that will be logged.

```
no level
```

Disables filtering of the log file by severity level.

Parameters

`debug`	Debug-level messages.
`info`	Informational messages.
`notice`	Normal, but significant condition.
`warning`	Warning conditions.
`error`	Error conditions.
`critical`	Critical conditions.
`alert`	Action must be taken immediately.
`emergency`	System is unusable.

level

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
level
```

Enables filtering of the log file by severity level.

```
no level
```

Disables filtering of the log file by severity level.

matches

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
matches (any | all) filters
```

All three log file filters (message, process, and level) are combined to filter the log according to this setting.

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
end
```

Switch to parent context.

inherit

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
inherit
```

Inherit settings from parent.

```
no inherit
```

Do not inherit setting from parent.

Provisioning connectivity context

Path: View > Enable > Controlled Network AP > Controlled Network > Provisioning connectivity
View > Enable > Controlled Network AP Group > Controlled Network > Provisioning connectivity
View > Enable > Controlled Network Base Group > Controlled Network > Provisioning connectivity

Set basic configuration for entity's provisioning connectivity.

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
end
```

Switch to parent context.

inherit

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
inherit
```

Inherit provisioning interface settings from parent.

```
no inherit
```

Do not inherit provisioning interface settings from parent.

interface

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
interface (port1 | local-mesh)
```

Set the provisioning interface.

interface provisioninig

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
interface provisioninig
```

Enable interface provisioning.

ip assignation

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
ip assignation (static | dhcp)
```

Set the ip assignment method.

vlan

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
vlan
```

Enable use of the provisioning vlan.

```
no vlan
```

Disable use of the provisioning vlan.

vlan

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`vlan <id>`

Set the provisioning vlan id.

`no vlan`

Disable use of the provisioning vlan.

static ip

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`static ip <ip> <netmask> <gateway>`

Set the static IP address.

provisioning local mesh group

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`provisioning local mesh group <id>`

Set the local mesh group id.

provisioning local mesh key

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`provisioning local mesh key <key>`

Set the local mesh security key.

provisioning local mesh port

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`provisioning local mesh port (radio1 | radio2)`

Set the radio used for local mesh .

provisioning local mesh security

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`provisioning local mesh security`

Enable the use of local mesh security.

`no provisioning local mesh security`

Disable the use of local mesh security.

provisioning local mesh security

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`provisioning local mesh security (wep | tkip | ccmp)`

Set the local mesh security mode.

```
no provisioning local mesh security
```

Disable the use of local mesh security.

provisioning local mesh type

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
provisioning local mesh type (a | b | g | bg)
```

Set the wireless mode for local mesh .

country code

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
country code <code>
```

Set the country code for local mesh .

Provisioning discovery context

Path: View > Enable > Controlled Network AP > Controlled Network > Provisioning discovery
View > Enable > Controlled Network AP Group > Controlled Network > Provisioning discovery
View > Enable > Controlled Network Base Group > Controlled Network > Provisioning discovery

Set basic configuration for entity's provisioning discovery.

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
end
```

Switch to parent context.

dns name

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
dns name <name>
```

Add a DNS name to the list.

```
no dns name <name>
```

Delete a DNS name from the list.

dns provisioning

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
dns provisioning
```

Enable DNS provisioning.

```
no dns provisioning
```

Disable DNS provisioning.

inherit

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
inherit
```

Inherit provisioning discovery settings from parent.

```
no inherit
```

Do not inherit provisioning discovery settings from parent.

dns domain name

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
dns domain name <name>
```

Set the DNS domain name.

dns server

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`dns server <ip>`

Add a DNS server to the list.

`no dns server <ip>`

Delete a DNS server from the list.

discovery provisioning

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`discovery provisioning`

Enable discovery provisioning.

`no discovery provisioning`

Disable discovery provisioning.

ip address

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`ip address <ip>`

Add an IP address to the list.

`no ip address <ip>`

Delete an IP address from the list.

ip provisioning

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`ip provisioning`

Enable IP provisioning.

`no ip provisioning`

Disable IP provisioning.

CN Wireless interface context

Path: View > Enable > Controlled Network AP > Controlled Network > CN Wireless interface
View > Enable > Controlled Network AP Group > Controlled Network > CN Wireless interface
View > Enable > Controlled Network Base Group > Controlled Network > CN Wireless interface

Configuration for controlled-mode wireless interfaces.

dot11

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`dot11 <mode> <frequency>`

Sets the wireless mode and the frequency the service controller will operate at.

Parameters

<mode> Sets the transmission speed and frequency band. The available options are determined by the wireless card installed in the service controller, and may include:

- a: Selects 802.11a providing 54 Mbps in the 5 GHz frequency band.
- b: Selects 802.11b providing 11 Mbps in the 2.4 GHz frequency band.
- g: Selects 802.11g providing 54 Mbps in the 2.4 GHz frequency band.
- bg: Selects 802.11b + 802.11g providing 11 and 54 Mbps in the 2.4 GHz frequency band.
- n: Selects 802.11n.
- an: Selects 802.11n + 802.11a, on the 5Ghz frequency band.
- gn: Selects 802.11n + 802.11g, on the 2.4Ghz frequency band.
- bgn: Selects 802.11n + 802.11g + 802.11b, on the 2.4Ghz frequency band.

<frequency> Sets the operating frequency by specifying a number in GHz or by specifying a channel number. The frequencies that are available are determined by the radio installed in the service controller and the regulations that apply in your country.

For optimum performance when operating in 802.11b or 802.11g modes, choose a frequency that differs from other wireless access points operating in neighboring cells by at least 25 MHz.

If operating in 802.11a mode, all channels are non-overlapping.

distance

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`distance (small | medium | large)`

Sets the distance between access points.

Use this parameter to adjust the receiver sensitivity of the service controller. This parameter should only be changed if:

- you have more than one wireless access point installed in your location
- you are experiencing throughput problems

In all other cases, use the default setting of Large.

If you have installed multiple service controllers, reducing the receiver sensitivity of the service controller from its maximum will help to reduce the amount of crosstalk between the wireless stations to better support roaming clients. By reducing the receiver sensitivity, client stations will be more likely to connect with the nearest access point.

transmit power

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
transmit power (DB | max)
```

Sets the maximum transmission power of the wireless radio.

Parameters

<db> Power is specified in steps of 1dBm. The maximum setting is 18 dBm.

Note: The actual transmit power used may less than the value specified. The service controller determines the power to used based on the settings you made for regulatory domain, wireless mode, and operating frequency.

multicast rate

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
multicast rate (1 | 2 | 5.5 | 6 | 9 | 11 | 12 | 18 | 24 | 36 | 48 | 54)
```

Sets the transmit rate for multicast traffic.

This is a fixed rate, which means that if a station is too far away to receive traffic at this rate, then the multicast will not be seen by the station. By rasing the multicast rate you can increase overall throughput significantly.

dot11 automatic frequency

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
dot11 automatic frequency
```

Enable this option to have the service controller automatically determine the best operating frequency.

```
no dot11 automatic frequency
```

Disable automatic frequency selection.

dot11 automatic frequency period

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
dot11 automatic frequency period (disabled | 1h | 2h | 4h | 8h | 12h | 24h)
```

Specify how often the frequency setting is re-evaluated when automatic frequency selection is enabled.

dot11 automatic frequency time

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
dot11 automatic frequency time <time>
```

Specify when the channel should be re-evaluated.

dot11 automatic transmit-power

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
dot11 automatic transmit-power
```

Enables automatic transmit power selection.

```
no dot11 automatic transmit-power
```

Disables automatic transmit power selection.

dot11 automatic transmit-power period

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
dot11 automatic transmit-power period (1h | 2h | 4h | 8h | 12h | 24h)
```

Sets the interval at which the transmit power setting is re-evaluated when automatic power selection is enabled.

antenna bidirectionnal

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
antenna bidirectionnal (diversity | main | auxiliary)
```

Sets the antenna to transmit and receive on. Select diversity to transmit and receive on both antennas.

Parameters

`diversity`	In this mode both antennas are used to transmit and receive. The service controller supports both transmit and receive diversity.
`main`	Transmit and receive on the main antenna only.
`aux`	Transmit and receive on the aux antenna only.

antenna gain

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
antenna gain <number>
```

Used only for Radar detection, records gain (in 5GHz band) of external antenna installed on device. Does not affect output power.

autochannel skip

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
autochannel skip <chan>
```

Adds the specified channel to the list of channels that are not allowed to be selected by the Auto Channel algorithm.

station distance

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
station distance (0km | 5km | 10km | 15km | 20km | 25km | 30km | 35km)
```

Fine tunes internal timeout settings to account for the distance that wireless links span. For normal operation, the AP is optimized for links of less than 1 km.

This is a global setting that is useful when creating wireless links to remote sites. However, it also applies to all wireless connection made with the radio, not just for wireless links. Therefore, if you are also using the radio to serve local wireless client stations, adjusting this setting may lower the performance for clients with marginal signal strength or when interference is present.
(Essentially, it means that if a frame needs to be retransmitted it will take longer before the actual retransmit takes place.)

beacon interval

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`beacon interval <value>`

Sets the beacon interval.

Parameters

< value>	Beacon interval value in the range 20 and 500 time units (TU) (1 TU = 1024us).

rts threshold

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`rts threshold <value>`

Sets the RTS threshold.

`no rts threshold`

Deletes the RTS threshold value.

Parameters

< value>	Threshold value in the range 128 and 1540.

Description

Use this parameter to control collisions on the link that can reduce throughput. If the Status Wireless page on the management tool shows increasing values for Tx multiple retry frames or Tx single retry frames, you should adjust this value until the errors clear up. Start with a value of 1024 and then decrease to 512 until errors are reduced or eliminated.

Using a small value for RTS threshold can affect throughput.

If a packet is larger than the threshold, the service controller will hold it and issue a request to send (RTS) message to the client station. Only when the client station replies with a clear to send (CTS) message will the service controller send the packet. Packets smaller than the threshold are transmitted without this handshake.

dot11 mode

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`dot11 mode (monitor | ap+wds | ap-only | wds-only | sensor)`

Sets the operating mode for the radio.

radio active

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`radio active`

Enables the radio.

```
no radio active
```

Disables the radio.

spectralink view

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
spectralink view
```

Enable the use of spectralink view.

```
no spectralink view
```

Disable the use of spectralink view.

dot11n guard interval

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
dot11n guard interval (short | long)
```

Select the 802.11n guard interval.

dot11n channel width

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
dot11n channel width (40 | 20 | auto)
```

Select the 802.11n channel width.

dot11n channel extension

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
dot11n channel extension (above | below)
```

Select the 802.11n channel extension. Applicable only in the 2.4 GHz band with a 40 MHz channel width.

dot11n multicast rate

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
dot11n multicast rate <rate>
```

Set the multicast rate for use with 802.11n networks.

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
end
```

Switch to parent context.

inherit

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
inherit
```

Inherit settings from parent.

```
no inherit
```

Do not inherit settings from parent.

RADIUS Profile context

Path: View > Enable > Controlled Network AP > Controlled Network > RADIUS Profile
View > Enable > Controlled Network AP Group > Controlled Network > RADIUS Profile
View > Enable > Controlled Network Base Group > Controlled Network > RADIUS Profile

Basic per entity RADIUS Profile configuration.

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
end
```

Switch to parent context.

inherit

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
inherit
```

Inherit settings from parent.

```
no inherit
```

Do not inherit settings from parent.

radius nas id

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
radius nas id <nasid>
```

Set the radius profile NAS Id.

Local mesh profile context

Path: View > Enable > Controlled Network AP > Controlled Network > Local mesh profile
View > Enable > Controlled Network AP Group > Controlled Network > Local mesh profile
View > Enable > Controlled Network Base Group > Controlled Network > Local mesh profile

Configuration for local mesh profiles.

security

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
security
```

Enables wireless security.

```
no security
```

Disables wireless security.

security mode

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
security mode (wep | tkip | ccmp)
```

Set the security mode.

security psk

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
security psk <secret>
```

Sets the PSK secret.

```
no security psk
```

Clears the PSK secret.

security wep

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
security wep <key>
```

Sets the WEP key.

```
no security wep
```

Deletes the WEP key.

dynamic mode

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
dynamic mode (master | alt-master | slave)
```

Selects the dynamic operation mode.

mesh id

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`mesh id <id>`

Set the local mesh group id.

allowed downtime

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`allowed downtime <number>`

Set the allowed downtime for a connection (or a link) to a peer.

minimum snr

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`minimum snr <number>`

Slave: Set the group's minimum SNR.

snr cost per hop

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`snr cost per hop <number>`

Slave: Set the group's SNR cost per hop.

initial discovery time

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`initial discovery time <number>`

Slave: Set the group's initial discovery time in seconds.

active

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`active`

Activates the local mesh group.

`no active`

Deactivates the local mesh group.

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`end`

Switch to parent context.

inherit

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`inherit`

Inherit settings from parent.

`no inherit`

Do not inherit settings from parent.

name

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`name <name>`

Renames the current local mesh group.

radio active

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`radio active (radio1 | radio2)`

Enables the radio.

`no radio active (radio1 | radio2)`

Disables the radio.

Local mesh provisioning profile context

Path: View > Enable > Controlled Network AP > Controlled Network > Local mesh provisioning profile
View > Enable > Controlled Network AP Group > Controlled Network > Local mesh provisioning profile
View > Enable > Controlled Network Base Group > Controlled Network > Local mesh provisioning profile

Configuration for local mesh provisioning profile.

accept connection

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
accept connection
```

Enable this group to act as alternate master.

```
no accept connection
```

Prevent this group from acting as alternate master.

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
end
```

Switch to parent context.

inherit

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
inherit
```

Inherit settings from parent.

```
no inherit
```

Do not inherit settings from parent.

multiple radio

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
multiple radio
```

On multiple radio products, use all available radios.

```
no multiple radio
```

On multiple radio products, do not use all available radios.

Switch port context

Path: View > Enable > Controlled Network AP > Controlled Network > Switch port
View > Enable > Controlled Network AP Group > Controlled Network > Switch port
View > Enable > Controlled Network Base Group > Controlled Network > Switch port

Switch port configuration.

Note
The commands in this context are used to perform configuration of the Ethernet switch built into the MSM317 Access Device.

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
end
```

Back to parent context.

active

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
active
```

Activate this port.

```
no active
```

Deactivate this port.

authentication profile vsc

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
authentication profile vsc <name>
```

Set the VSC (Virtual AP) to use for authentication.

```
use authentication profile vsc
```

Use the VSC (Virtual AP) for authentication.

```
no use authentication profile vsc
```

Ignore the VSC (Virtual AP) for authentication.

authentication server radius

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
authentication server radius <name>
```

Select RADIUS profile to use.

dot1x authentication

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
dot1x authentication
```

Enable support for IEEE802.1X.

```
no dot1x authentication
```

Disable support for IEEE802.1X.

dynamic vlan

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
dynamic vlan
```

Enable dynamic VLAN.

```
no dynamic vlan
```

Disable dynamic VLAN.

egress rate

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
egress rate <(128k|256k|512k|1m|2m|4m|8m|16m|32m)>
```

Set the maximum rate at which this port will accept egress traffic.

```
use egress rate
```

Limit the egress data rate.

```
no use egress rate
```

Do not limit the egress data rate.

force flow control

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
force flow control
```

Force flow control on this port.

```
no force flow control
```

Do not force flow control on this port.

ingress rate

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
ingress rate <(128k|256k|512k|1m|2m|4m|8m|16m|32m)>
```

Set the maximum rate at which this port will accept ingress traffic.

```
use ingress rate
```

Limit the ingress data rate.

```
no use ingress rate
```

Do not limit the ingress data rate.

ingress traffic type

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
ingress traffic type (broadcast | multicast+broadcast | all)
```

Select the type of traffic to which rate limiting applies.

mac authentication

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
mac authentication
```

Enable support for MAC-based authentication.

```
no mac authentication
```

Disable support for MAC-based authentication.

mac filter list

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
mac filter list <name>
```

Accept MAC addresses set in these lists.

```
no mac filter list <name>
```

Remove this list of MAC ranges.

port name

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
port name <name>
```

Change the port name.

port type

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
port type (tagged | untagged)
```

Configure the port type.

power over ethernet

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
power over ethernet
```

Use PoE on this port.

```
no power over ethernet
```

Do not use PoE on this port.

priority

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
priority (low | medium | high | very-high)
```

Set the default QoS priority for this port.

priority lookup

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
priority lookup (diffsrv | 802.1p | any)
```

Choose the port priority lookup.

```
use priority lookup
```

Turn on priority lookup for this port.

```
no use priority lookup
```

Turn on priority lookup for this port.

quarantine vlan

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
quarantine vlan <number>
```

Set the quarantine VLAN ID.

```
no quarantine vlan
```

Clear the quarantine VLAN.

```
use quarantine vlan
```

Use the quarantine VLAN setting.

```
no use quarantine vlan
```

Do not use the quarantine VLAN setting.

vlan

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

```
vlan <number>
```

Set the VLAN ID for this port.

```
use vlan
```

Apply the VLAN.

```
no use vlan
```

Do not apply the VLAN.

List of MAC addresses context

Path: View > Enable > Config > List of MAC addresses

Use to modify a list of MAC addresses.

end

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`end`

Go to previous context.

entry

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`entry <mac>`

Adds a new entry to the list.

`no entry <mac>`

Removes the entry from the list.

list name

Supported on: MSM710 MSM730 MSM750 MSM760 MSM765zl

`list name <string>`

Change the current list name.

Technology for better business outcomes

To learn more, visit www.hp.com/go/procurve/

May 2009

Manual Part Number
5992-5933